Fast and Simple One-Way High-Dimensional Quantum Key Distribution

Kfir Sulimany[1], Rom Dudkiewicz[2], Simcha Korenblit[1], Hagai S. Eisenberg[1], Yaron Bromberg[1 *], and Michael Ben-Or[2 *]

[1]Racah Institute of Physics, The Hebrew University of Jerusalem, Jerusalem 91904, Israel
[2]School of Computer Science & Engineering, The Hebrew University of Jerusalem, Jerusalem, 91904 Israel
[*]Corresponding authors: yaron.bromberg@mail.huji.ac.il, benor@cs.huji.ac.il

Abstract

High-dimensional quantum key distribution (QKD) provides ultimate secure communication with secure key rates that cannot be obtained by QKD protocols with binary encoding. However, so far the proposed protocols required additional experimental resources, thus raising the cost of practical high-dimensional systems and limiting their use. Here, we analyze and demonstrate a novel scheme for fiber-based arbitrary-dimensional QKD, based on the most popular commercial hardware for binary time bins encoding. Quantum state transmission is tested over 40 km channel length of standard single-mode fiber, exhibiting a two-fold enhancement of the secret key rate in comparison to the binary Coherent One Way (COW) protocol, without introducing any hardware modifications. This work holds a great potential to enhance the performance of already installed QKD systems by software update alone.

1 Introduction

Quantum key distribution (QKD) is an advanced technology which provides ultimate secure communication by exploiting quantum states of light as information carriers over communication channels [1, 2, 3]. In the early QKD protocols each bit of the key was encoded using a quantum state belonging to a binary Hilbert space [4, 5]. High-dimensional QKD protocols were introduced more recently, based on preparing a set of states belonging to a d-dimensional Hilbert space, called qudits [6, 7]. The higher information capacity of qudits allows a higher secure key rate and improves the robustness to the noise, leading to higher threshold values of the quantum bit error rate (QBER) [8].

Time-bin encoding of weak coherent laser pulses is the most popular technique for implementing QKD over single-mode fibers [9, 10, 11]. Recent demonstrations of high-dimensional temporal encoding showed a significant key rate improvement [12, 13, 14]. In particular, a record-breaking key rate of 26.2 Mbit/s was achieved with a four-dimensional time-bin protocol that is robust against the most general (or coherent) attacks [12].

However, implementation of high-dimensional QKD protocols in commercial systems is still held back, since present high-dimensional schemes require significantly higher experimental resources. The large experimental overhead results from the fact that high-dimensional encoding not only increases the channel capacity, but it also increases the amount of information that Eve can extract. Most QKD protocols limit the amount of information accessible to Eve by projecting the quantum states at the receiver's end on unbiased bases. While the projection in binary schemes is usually implemented with a single interferometer followed by a single photon detector (SPD), most d-dimensional schemes require $O(d)$ imbalanced interferometers and $O(d)$ SPDs. Thus, to date, all high-dimensional QKD systems implementations required complex and expensive systems that are impractical for commercial applications.

In this work we present a different approach for high-dimensional QKD with time-bin encoding, which can be implemented using a standard commercial QKD system without any hardware modifications. Instead, we show that Eve's information can be bounded by simply randomizing the time-bins order. We further analyze the security and expected secure key rate for optimized Eve's strategy. Finally, we experimentally demonstrate a 32 dimensional protocol over a 40 km long fiber using only two single-photon detectors and one interferometer at the receiver end. We demonstrate the improved performance of our protocol in comparison to the binary COW protocol using the same experimental setup, and show more than a two-fold increase in the asymptotically secure key rate.

2 Protocol Scheme

Our high-dimensional protocol is based on the coherent one-way (COW) QKD protocol, where the bit string is encoded in the time of arrival of weak coherent laser pulses and the channel disturbance is monitored by measuring the visibility of the interference between neighbouring pulses [15]. That is, bits 0 and 1 are sent using $|\alpha\rangle|0\rangle$ and $|0\rangle|\alpha\rangle$, respectively, where $|0\rangle$ is the vacuum and $|\alpha\rangle$ is a coherent state. On Bob's side, he simply recovers the bit value by measuring the arrival time of the laser pulse. To detect attacks, a small fraction of the pulses splits to a monitoring line by a fiber beam splitter. In the monitoring line Bob checks for phase coherence between any two successive laser pulses by using an imbalanced interferometer and one single photon detector.

Our extension to a high dimension is based on a more efficient utilization of the quantum bit duration relative to the deadtime of the detector which limits the number of bits that can be received per second. The qudits of the raw key are encoded as time slot sequences where in each sequence one of the slots is populated and the others are empty. Some sequences are gathered to a block and permuted randomly to create a permuted key block as shown in Figure 1. Then, the block is converted to occupied and non occupied pulse sequence. The important feature caused by the permutation is that two successive occupied pulses can originate anywhere in the raw key block. This randomization enables us to bound Eve's information and extract higher secure key rate although the monitoring mechanism works in the same way as the binary protocol.

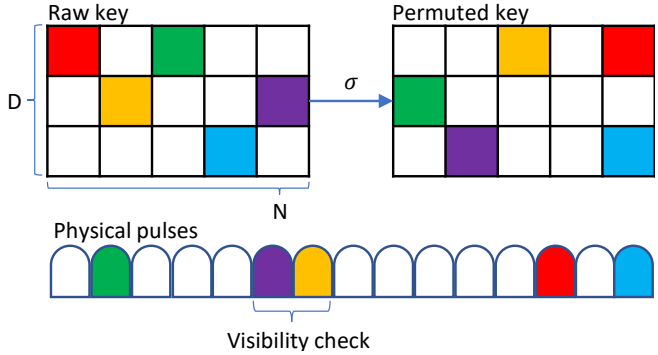

Figure 1: **Protocol scheme** Alice produces a secret key consisting of a block of N/D random numbers where D is the dimensional encoding. She permutes the block with a random secret permutation to get a scrambled block, and transmits accordingly a series of occupied and empty pulses. This way, a pair of sequentially occupied pulses can originate from any two time slots in the raw key block, an important feature of the protocol that is essential for the security proof.

3 Security Analysis

We now turn to explain the protocol in details, present the encoding states and Eve's strategy, and compute the Holevo information and the number of secure bits per photon. AS our protocol is a variation on the binary COW protocol, we follow the analysis tools presented in [16]. Alice and Bob work in blocks, communicating n qudits at a time, each of dimension d. Let $q_0, ..., q_{n-1} \in \{1...d\}$ be the raw key Alice wants to transmit. Alice chooses a random permutation σ of $\{1...d{\cdot}n\}$ and over the next $d{\cdot}n$ time bins sends $|\alpha\rangle$ at time slot t if t=$\sigma(d{\cdot}i+q_i)$ for some i in {0...n-1} and $|0\rangle$ otherwise as illustrated in Figure 1. After Bob measures the pulse sequence, Alice transmits σ over the classical channel. When Bob detects a click at time t, he calculates $\sigma^{-1}(t) = i \cdot d + j \ for \ i \in \{0...n-1\} \ and \ j \in \{1...d\}$ meaning the value passed in the i'th qudit was j. Bob transmits back to Alice which qudits he received, such that the information in them is now mutual up to error correction. The monitoring line works the same as the regular COW protocol, using an imbalanced interferometer to measure the coherence between consecutive pulses for a small percentage of the pulses.

In principle, Eve can act on a small blocks of signals each time. However, if Alice and Bob use large blocks ($n \gg 1$), Eve cannot differentiate between qudits, as statistically each signal in the qudit is averaged by Eve's actions whenever it is in different positions in Eve's block and different neighbouring signals. We can look at Eve's action as a linear transformation [16]

$$|0\rangle_A|\varepsilon\rangle_E \rightarrow |0\rangle_B|v_0\rangle_E + \sqrt{Q\mu t}|1\rangle_B|p_0\rangle_E \tag{1}$$

$$|\sqrt{\mu}\rangle_A|\varepsilon\rangle_E \rightarrow |0\rangle_B|v_\mu\rangle_E + \sqrt{(1-(d-1)Q)\mu t}|1\rangle_B|p_\mu\rangle_E. \tag{2}$$

Assuming Eve's actions does not add any noise, Eve's action has three main constraints: i) It must be unitary, thus $\langle v_0|v_\mu\rangle = e^{-\mu/2}$. ii) It must retain the QBER, which is already represented in the equations. iii) It must keep the visibility. Neglecting two-photon terms and under the assumption that $\mu t \ll 1$, Eve's action on $|\sqrt{\mu}\rangle|\sqrt{\mu}\rangle$ is given by

$$\begin{aligned} &|0,0\rangle_B|v_\mu, v_\mu\rangle_E \\ &+\sqrt{(1-(d-1)Q)\mu t}[|1,0\rangle_B|p_\mu, v_\mu\rangle_E \\ &+|0,1\rangle_B|v_\mu, p_\mu\rangle_E]. \end{aligned} \tag{3}$$

The visibility condition then yields $V = Re[\langle p_\mu, v_\mu|v_\mu, p_\mu\rangle] = |\langle p_\mu|v_\mu\rangle|^2$.

We are interested in Eve's information, for which we will observe the result of her action on a qudit, and calculate the Holevo information. Eve's action, after neglecting all multiple photon terms, can be presented as:

$$
\begin{aligned}
&|0,...,0,\sqrt{\mu}^{(i),0,...,0}\rangle|\varepsilon,...,\varepsilon\rangle \rightarrow \\
&|0,...,0\rangle \otimes V_i \\
&+\sqrt{(1-(d-1)Q)\mu t}|0,...,0,1^{(i)},0...,0\rangle \otimes C_i \\
&+\sum_{k=1...d,k\neq i} \sqrt{Q\mu t}|0,...,0,1^{(k)},0...,0\rangle W_{i,k}
\end{aligned} \tag{4}
$$

where $V_i = |v_0,...,v_0,v_\mu^{(i)},v_0,...,v_0\rangle$ is Eve's state for passing void, $C_i = |v_0,...,v_0,p_\mu^{(i)},v_0,...,v_0\rangle$, is Eve's state for passing the qudit information correctly as i, and $W_{i,k} = |v_0,...,v_0,p_0^{(k)},v_0,...,v_0,v_\mu^{(i)},v_0,...,v_0\rangle$ is Eve's state for passing the wrong information, k instead of i.

The state of Eve's subsystem, given a detection and depending on Alice or Bob's bit, is given by

$$
\begin{aligned}
\rho_E^{A=i} &= (1-(d-1)Q)|C_i\rangle\langle C_i| \\
&+\sum_{k=1...d,k\neq i} Q|W_{i,k}\rangle\langle W_{i,k}|
\end{aligned} \tag{5}
$$

$$
\begin{aligned}
\rho_E^{B=i} &= (1-(d-1)Q)|C_i\rangle\langle C_i| \\
&+\sum_{k=1...d,k\neq i} Q|W_{k,i}\rangle\langle W_{k,i}|
\end{aligned} \tag{6}
$$

We now look at Eve's Holevo information,

$$
\chi_{AE} = S(\sum_{i=1...d}\frac{1}{d}\rho_E^{A=i}) - \sum_{i=1...d} S(\frac{1}{d}\rho_E^{A=i}) \tag{7}
$$

Eve has no constraints over p_0 and thus can choose it to be orthogonal to all other vectors (v_0, v_μ, p_μ) to maximize her information. We can separate the trace of the above matrices by those having p_0 at a certain index and those not, yielding

$$
\begin{aligned}
\chi_{AE} = &\sum_{k=1...d}\left[s\left(\sum_{i=1...d-1}\frac{Q}{d}|V_i'\rangle\langle V_i'|\right)\right. \\
&\left.-\frac{1}{d}S\left(\sum_{i=1...d-1}Q|V_i'\rangle\langle V_i'|\right)\right] \\
&+s\left(\sum_{i=1...d}\frac{1-(d-1)Q}{d}|C_i\rangle\langle C_i|\right) \\
&-\frac{1}{d}\sum_{i=1...d} S\left((1-(d-1)Q)\,|C_i\rangle\langle C_i|\right)
\end{aligned} \tag{8}
$$

Such that $V_i' = \overbrace{|v_0,...,v_0,v_\mu^{(i)},v_0,...,v_0\rangle}^{d-1\ terms}$ so that $V_i' \otimes p_0 = W_{i,d}$ and equivalent up to reordering the base to $W_{i,j}$ for different j.

After diagonalization and summation, we obtain the following expression for the Holevo information:

$$
\begin{aligned}
\chi_{AE} = &\, d\cdot s\left(\frac{Q}{d}\left((d-2)e^{-\mu}+1\right)\right) \\
&+d(d-2)s\left(\frac{Q}{d}\left(1-e^{-\mu}\right)\right) \\
&-s\left(Q\left((d-2)e^{-\mu}+1\right)\right) \\
&-(d-2)s\left(Q\left(1-e^{-\mu}\right)\right) \\
&+s\left(\frac{1-(d-1)Q}{d}\left((d-1)\langle v_0|p_\mu\rangle^2+1\right)\right) \\
&+(d-1)s\left(\frac{1-(d-1)Q}{d}\left(1-\langle v_0|p_\mu\rangle^2\right)\right) \\
&-S\left(1-(d-1)Q\right)
\end{aligned} \tag{9}
$$

and similarly for Bob:

$$
\begin{aligned}
\chi_{BE} = &\, d\cdot s\left(\frac{Q}{d}\left((d-2)e^{-\mu}+1\right)\right) \\
&+d(d-2)s\left(\frac{Q}{d}\left(1-e^{-\mu}\right)\right) \\
&-(d-1)s\left(Q\right) \\
&+s\left(\frac{1-(d-1)Q}{d}\left((d-1)\langle v_0|p_\mu\rangle^2+1\right)\right) \\
&+(d-1)s\left(\frac{1-(d-1)Q}{d}\left(1-\langle v_0|p_\mu\rangle^2\right)\right) \\
&-S\left(1-(d-1)Q\right)
\end{aligned} \tag{10}
$$

We analytically maximize the Holevo information to determine the secure key rate. The information passed per qudit thus equals

$$
\begin{aligned}
I_{AB} = &\log_2(d) + (d-1)Q\log_2(Q) + \\
&(1-(d-1)Q)\log_2\left(1-(d-1)Q\right) - \chi_{BE}
\end{aligned} \tag{11}
$$

One of the caveats of high dimension qudits is that the time per qudit sent is longer . In practice, the time per received qudit is limited by the deadtime of the detector. To calculate the received bit rate we write the clicks per time as $clicks(t) = \alpha t$, where t denotes time. For each pulse, either it will be undetected and we get remaining clicks from the time after the pulse (τ) or it will be detected, which will give us a click, plus all the clicks after the detector's deadtime(T) such that $clicks(t) = P(click)(1+clicks(t-T-\tau))+(1-P(click))clicks(t-\tau)$ the chance for a click, is the chance of a pulse being fired $frac1D$ for D the qudit dimension, times the detector efficiency ξ time the occupation μ so we get

$$
\alpha t = \frac{\xi\mu}{D}(1+\alpha(t-T-\tau)) + (1-\frac{\xi\mu}{D})\alpha(t-\tau) \tag{12}
$$

from which we can extract

$$
\alpha = \frac{\frac{\xi\mu}{D}}{(T+\tau)\frac{\xi\mu}{D}+\tau(1-\frac{\xi\mu}{D})} = \frac{1}{T+\tau\frac{D}{\xi\mu}} \tag{13}
$$

and when we look at the total secure key rate per second it will be αI_{AB}.

4 Experimental Implementation

The important feature of our high-dimensional protocol is that it is implemented in a standard binary COW system as depicted in figure 2 without any hardware changes. The system consists of a transmitter (Alice) and a receiver (Bob). The transmitter sends a train of weak coherent pulses that are prepared from a continuous wave (CW) laser emitting at $\lambda = 1550nm$, by an intensity modulator (IM) running at $500MHz$. Before leaving the transmitter, the pulses are attenuated to reach single photon level using a variable optical attenuator (VOA). To generate $200ps$ long pulses with random occupations of $\tau = 2ns$ long time-bins we use field programmable gate array (FPGA). Synchronization is achieved over the 40 km fiber channel using the White Rabbit protocol [17]. To interfere consecutive pulses at the receiver's end, a fiber unbalanced Michelson interferometer is installed, where we use Faraday mirrors to compensate for random polarization drifts in the fiber interferometer (figure 2 (b)). We use single-photon avalanche detectors (SPADs) with 20% detection efficiency and $400ps$ timing resolution. The detectors' dead time is $4\mu s$ limits the maximal raw key rate to $250kHz$.

We analyze the performance of the protocol for different dimension sizes, and compare the experimental results obtained with our QKD system with the predictions of a cleaner theoretical model. We first calculate the number of secure bits per photon as a function of the pulse occupation for different dimensions, as presented in Figure 3a. Solid lines present the number of secure bits per photon for our syste, based on the measured QBER and visibility for each dimensional encoding size. The dashed lines present the calculated secure bits per photon for the theoretical model, where we assumed visibility of 99% and a QBER of 0.4% per time slot. Here we also assumed the QBER scales linearly with the dimension size. The main source for such linear scaling is the finite extinction ratio of the intensity modulator, typically on the order of 0.01. In the limit of low occupation, the deterors' dark counts may become the dominate source for linear scaling of the QBER with the dimension size.

As appears in Figure 3a, higher dimensional encoding allows higher secure bits per photon. At teh same time, increasing the pulse occupation weakens the constraints on Eve and therefore increases the information she can obtain, decreasing the number of secret bits per photon. In Figure 3 b) we present the number of detected photons per second versus the pulse occupation, for different dimensions. The solid lines present the measured number of detected photons per second, and the dashed lines present the calculated detection as in Equation 13: $\frac{1}{T+\tau\frac{D}{\xi\mu}}$. The number of raw bits per photon increase linearly up to occupation of around 5% where the detector saturates. In Figure 3 c) we present the secure bits per second, obtained by multiplying the raw bits per photon by the number of detected photons per second. An optimal secure bit rate is achieved for D=8, resulting in more than a two-fold increase in the secure bits rate for both the experimental data and for the theoretical model.

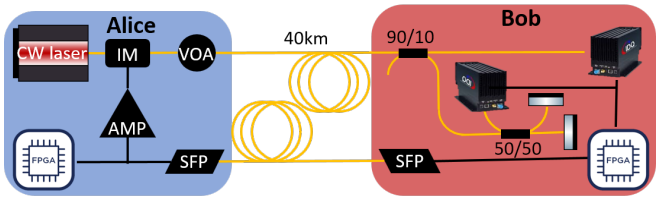

Figure 2: **Experimental setup for comparing arbitrary-dimensional QKD schemes.** Alice's transmitter (left) consists of a continuous wave (CW) laser at $\lambda = 1550nm$ that is modulated using an electro-optic intensity modulator (IM) running at $500MHz$ before passing through a variable optical attenuator (VOA) that regulates the mean photon number per pulse. The weak coherent pulses are delivered to Bob's end through a $40km$ long SMF-28 fiber. Bob's receiver (right) consists of an asymmetric beamsplitter, which provides a passive choice of the measurement basis. After the beamsplitter the photons either travel directly to the data detector, or pass through an unbalanced interferometer and detected by the monitor detector. We lock the laser's wavelength to the interferometer so that the monitor detector always measures the dark port of the interferometer. The interference visibility is estimated by registering the detection events due to the interfering and non-interfering events. In addition to the $40km$ long quantum channel that delivers the weak coherent pulses, we use a separate $40km$ SMF-28 fiber for all classical communication between Alice and Bob and to distribute an optical clock signal between them based on he White Rabbit protocol [17]. State preparation and sifting is run by two field-programmable gate arrays (FPGA) at Alice's and Bob's ends.

While the experimental results and theoretical model exhibit similar trends, the model fails to capture the exact secure bit rate, due to the oversimplification of the model that assume linear scaling of the QBER with the dimension size. In practice, one of the main noise sources in fast modulation transmitters is cross-talk between consecutive pulses, due to electronic ringing. Since higher dimensions result in longer average times between consecutive pulses, the sensitivity to cross-talk between consecutive pulses decreases with the dimension size. Thus in our system he experimentally measured QBER per encoding time bin decrease as the dimension is increased (Figure 4), yielding higher secure bit rates than the model's prediction.

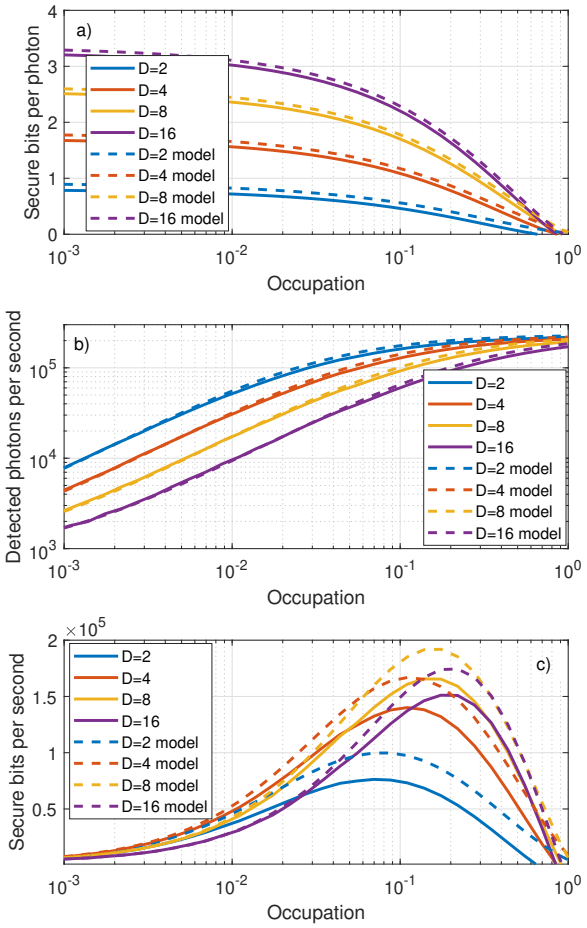

Figure 3: **Key rates for different dimensions.** a) Number of secure bits per photon (solid) for our system and for the model system (dashed). Increasing the pulse occupation weakens the constraints on Eve and therefore increases the information she can obtain, yielding a lower nuber of secure bits per photon. Higher dimensional encoding allows a higher number of secure bits per photon. b) Number of raw bits per photon in our system (solid) and the calculated raw bits per second for the model system. c) Secure bits per second is the multiplication of the raw bits per photon by photons per second. The optimum is achieved at $D = 8$, where the number of secure bits per second increases by 2.16 for our system, and by 1.97 for the model.

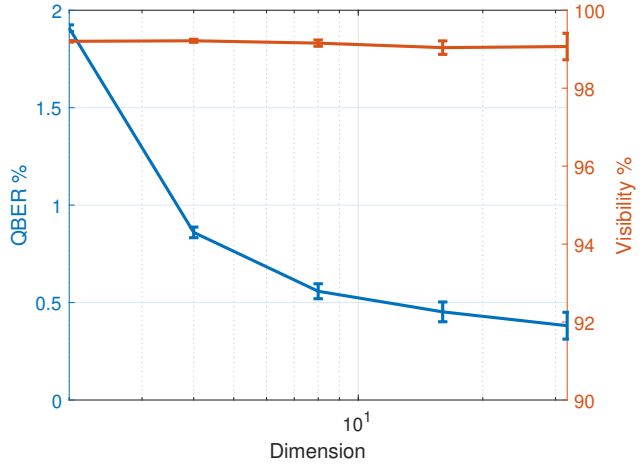

Figure 4: **QBER and visibility as a function of the protocol's dimension.** The QBER per encoding time bin decreases with the dimension size, due to electronic ringing common in high-rate modulation systems. The measured visibility is insensitive to the dimension size. Error bars are calculated assuming shot-noise limited detection.

5 Discussion

A major disadvantage of our protocol is that it does not exhibit higher resilience to noise as expected from high-dimensional QKD protocols. We calculate the secure key rate per photon versus the bit error rate for different dimensional encoding sizes as presented in Figure 5. In the case of $D = 2$ we were able to extract secure key rate up to QBER of 13.6%, while for $D = 16$ the maximal QBER the protocol can tolerate reduces to 6.2%. This is caused by the linear scaling of the error rate with the dimension due to the leakage of the modulator and the dark counts. Our protocol is therefore not optimal for increasing the communication distances. Fortunately, however, our protocol is useful in most commerciallt relevant cases since in realistic systems the typical error rate is lower than a few percent.

So far we focused on the most popular and cost effective commercial design based on standard single photon APDs and showed a significant enhancement of the secure bit rate. A Similar analysis shows an improvement also for high-end QKD systems based on superconducting nanowire detectors. For example, considering $100ns$ dead time and modulation rates as high as $10Gbps$, the secure bit rate at dimension $D = 8$ may increase by a factor of 1.66 at relative to standard binary COW encoding.

6 Conclusion

In conclusion, we present an arbitrary high-dimensional QKD protocol, supported by a security proof, which has the advantage of requiring only standard binary QKD hardware. This scheme is experimentally tested with a standard binary encoding system and its performance is compared between protocols with different dimension sizes. We demonstrate more than a two-fold enhancement of the secure key rate in the saturation regime of

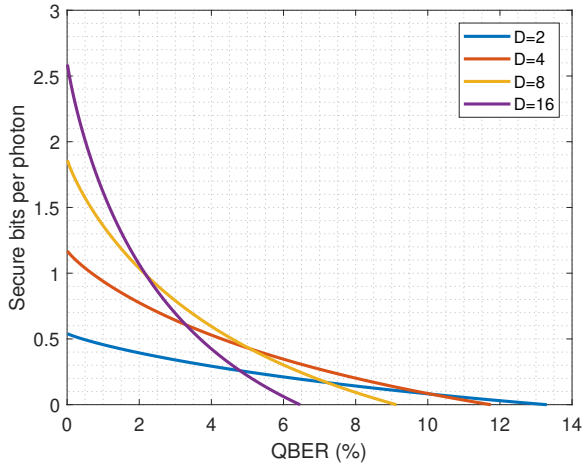

Figure 5: **Secret key rate per photon as function of the bit error rate for dimensions D = 2, 4, 8, 16.** The binary case is the most robust to noise. Increasing the dimension decreases the maximal QBER that allows positive secure key rate per photon.

APD detectors. Our demonstration proves that high-dimensional quantum systems allow a significant improvement in the key generation process as compared with the binary-encoding case. At the same time, no extra resources are necessary for the full implementation of such a system. Moreover, the protocol is not limited to time-bins encoding. For example, generalizing spatial encoding based on non overlapping Gaussian beams is possible with one Michelson interferometer. Thus, our experiment paves the way towards software update of installed QKD systems and a wider use of high-dimensional encoding in quantum communication.

Acknowledgements

This research was supported by the *United States-Israel Binational Science Foundation (BSF)* (Grant No. 2017694). KS and YB acknowledge the support of the Israeli Council for Higher Education and Technology and the Zuckerman STEM Leadership Program.

References

[1] Charles H Bennett and David P DiVincenzo. "Quantum information and computation". In: *nature* 404.6775 (2000), pp. 247–255.

[2] Nicolas Gisin et al. "Quantum cryptography". In: *Reviews of modern physics* 74.1 (2002), p. 145.

[3] Stefano Pirandola et al. "Advances in quantum cryptography". In: *Advances in Optics and Photonics* 12.4 (2020), pp. 1012–1236.

[4] Charles H Bennett and Gilles Brassard. *Proceedings of the ieee international conference on computers, systems and signal processing*. 1984.

[5] Artur K Ekert. "Quantum cryptography based on Bell's theorem". In: *Physical review letters* 67.6 (1991), p. 661.

[6] Helle Bechmann-Pasquinucci and Wolfgang Tittel. "Quantum cryptography using larger alphabets". In: *Physical Review A* 61.6 (2000), p. 062308.

[7] Nicolas J Cerf et al. "Security of quantum key distribution using d-level systems". In: *Physical review letters* 88.12 (2002), p. 127902.

[8] Daniele Cozzolino et al. "High-Dimensional Quantum Communication: Benefits, Progress, and Future Challenges". In: *Advanced Quantum Technologies* 2.12 (2019), p. 1900038.

[9] Boris Korzh et al. "Provably secure and practical quantum key distribution over 307 km of optical fibre". In: *Nature Photonics* 9.3 (2015), pp. 163–168.

[10] Alberto Boaron et al. "Secure quantum key distribution over 421 km of optical fiber". In: *Physical review letters* 121.19 (2018), p. 190502.

[11] Beatrice Da Lio et al. "Experimental demonstration of the DPTS QKD protocol over a 170 km fiber link". In: *Applied Physics Letters* 114.1 (2019), p. 011101.

[12] Nurul T Islam et al. "Provably secure and high-rate quantum key distribution with time-bin qudits". In: *Science advances* 3.11 (2017), e1701491.

[13] Nurul T Islam et al. "Scalable high-rate, high-dimensional time-bin encoding quantum key distribution". In: *Quantum Science and Technology* 4.3 (2019), p. 035008.

[14] Ilaria Vagniluca et al. "Efficient time-bin encoding for practical high-dimensional quantum key distribution". In: *Physical Review Applied* 14.1 (2020), p. 014051.

[15] Damien Stucki et al. "Fast and simple one-way quantum key distribution". In: *Applied Physics Letters* 87.19 (2005), p. 194108.

[16] Cyril Branciard, Nicolas Gisin, and Valerio Scarani. "Upper bounds for the security of two distributed-phase reference protocols of quantum cryptography". In: *New Journal of Physics* 10.1 (2008), p. 013031.

[17] Maciej Lipiński et al. "White rabbit: A PTP application for robust sub-nanosecond synchronization". In: *2011 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control and Communication*. IEEE. 2011, pp. 25–30.