Simple and high-speed polarization-based QKD

Fadri Grünenfelder, Alberto Boaron, Davide Rusca, Anthony Martin, and Hugo Zbinden

Citation: Appl. Phys. Lett. **112**, 051108 (2018);
View online: https://doi.org/10.1063/1.5016931
View Table of Contents: http://aip.scitation.org/toc/apl/112/5
Published by the American Institute of Physics

Simple and high-speed polarization-based QKD

Fadri Grünenfelder, Alberto Boaron,[a] Davide Rusca, Anthony Martin, and Hugo Zbinden
Group of Applied Physics, University of Geneva, Chemin de Pinchat 22, CH-1211 Geneva 4, Switzerland

(Received 22 November 2017; accepted 14 January 2018; published online 31 January 2018)

We present a simplified BB84 protocol with only three quantum states and one decoy-state level. We implement this scheme using the polarization degree of freedom at telecom wavelength. Only one pulsed laser is used in order to reduce possible side-channel attacks. The repetition rate of 625 MHz and the achieved secret bit rate of 23 bps over 200 km of standard fiber are the actual state of the art. *Published by AIP Publishing*. https://doi.org/10.1063/1.5016931

Secure communication is a central pillar of today's society, playing a key role not only in finance, defence, and industry but also in the protection of the privacy of individuals. Most cryptographic systems used at present, however, are lacking an information theoretical security proof and are threatened by future quantum computers. Quantum key distribution (QKD) offers a way to overcome this security issue by exchanging a secret key over an insecure optical link. This key can be used in the One-Time-Pad for secure communication.[1]

The idea of QKD was born in 1984 when Bennett and Brassard proposed a protocol which is now known as BB84.[2] Nowadays, a variety of different protocols exist and many implementations using different degrees of freedom (DoF) of photons (polarization, phase, etc.) have been demonstrated using optical fibers or free-space.[3–8]

For practical reasons, implementations of polarization-based BB84 often use weak pulses from several different laser diodes, one for each qubit state.[9–12] However, different lasers may have slightly different properties such as frequency and emission time, offering to an eavesdropper Eve the possibility of a so-called side-channel attack. Eve, by looking at those properties, may determine the qubit states sent without disturbing them.[13,14]

In this paper, we present a complete polarization-based QKD setup based on a single laser in order to prevent side-channel attacks exploiting the distinguishability of different lasers. The source works at a repetition rate of 625 MHz. We reduce the complexity of the scheme as much as possible, using a three-state protocol,[15] only one decoy-state level,[16,17] and only two single-photon detectors. We perform a complete key exchange, with real-time error correction and privacy amplification based on finite-key analysis.

In the following, we describe the protocol step by step.

1. **State preparation:** Alice uses a laser source emitting phase-randomized weak coherent pulses and encodes the states in the polarization DoF of the photons. She chooses randomly one of the two bases X or Z with the associated probabilities $p_{\mathsf{X}}^{\mathrm{A}}$ and $p_{\mathsf{Z}}^{\mathrm{A}} = 1 - p_{\mathsf{X}}^{\mathrm{A}}$, respectively. In the basis Z, she generates with uniform probability the state $|H\rangle$ or $|V\rangle$. In the basis X, she just prepares $|+\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$. The pulse energy is chosen at random among one of the two mean photon numbers μ_1 and μ_2 with the constraint $\mu_1 > \mu_2 > 0$ and probabilities p_{μ_1} and $p_{\mu_2} = 1 - p_{\mu_1}$, respectively. μ_1 is denoted as the signal level, while μ_2 is the decoy level. Alice sends the qubits through an optical fiber to Bob.
2. **Measurement:** Bob performs a measurement on the incoming signal at random in one of the two bases X or Z with respective probabilities $p_{\mathsf{X}}^{\mathrm{B}}$ and $p_{\mathsf{Z}}^{\mathrm{B}} = 1 - p_{\mathsf{X}}^{\mathrm{B}}$. For each detection, the basis and the measurement result are recorded.
3. **Basis reconciliation:** Alice and Bob announce their basis settings for the events where a detection has occurred. The events from the Z basis are used to generate the raw key, while those from the X basis are used to estimate the eavesdropper potential information. After having collected $n_{\mathsf{Z}}^{\mathrm{EC}}$ new raw key bits, they continue with step 4.
4. **Error correction:** Alice and Bob apply an error correction algorithm on the block of $n_{\mathsf{Z}}^{\mathrm{EC}}$ bits during which $\lambda_{\mathrm{EC}} = f_{\mathrm{EC}} \cdot n_{\mathsf{Z}}^{\mathrm{EC}} \cdot h(Q_{\mathsf{Z}})$ bits are disclosed where f_{EC} is the efficiency of reconciliation, $h(x)$ the binary entropy, and Q_{Z} the error rate. In our protocol, we employed the error correction algorithm Cascade which has a reconciliation efficiency around 1.06.[18] The procedure succeeds with a probability $1 - \epsilon_{\mathrm{corr}}$. After $k = n_{\mathsf{Z}}/n_{\mathsf{Z}}^{\mathrm{EC}}$ error correction blocks, they proceed to step 5.
5. **Privacy amplification:** Alice and Bob apply the privacy amplification procedure on a block of size n_{Z} to obtain a secret key of l bits.[19] l is upper bounded by

$$l \leq s_{\mathsf{Z},0} + s_{\mathsf{Z},1}(1 - h(\phi_{\mathsf{Z}})) - \lambda_{\mathrm{EC}}^{t} - 4\log_2(7/\epsilon_{\mathrm{sec}}) - \log_2(1/\epsilon_{\mathrm{cor}}), \quad (1)$$

where $s_{\mathsf{Z},0}$ and $s_{\mathsf{Z},1}$ are the lower bound on the number of vacuum and single-photon detection in the Z basis, ϕ_{Z} is the upper bound on the phase error rate, $\lambda_{\mathrm{EC}}^{t}$ is the total number of bits revealed during the error correction, and ϵ_{sec} and ϵ_{cor} are the secrecy and correctness parameters, respectively.

Having only two intensity levels does not allow us to directly measure an upper bound on $s_{\mathsf{Z},0}$, which is necessary to estimate the lower bound on the single-photon events. To solve this issue, we consider that the total number of errors on each basis is only due to the vacuum component. This is the most conservative way to estimate the upper bound of $s_{\mathsf{Z},0}$ (for more details, see Ref. 20).

Now, we describe the experimental setup that is shown in Fig. 1. The experiment is controlled by two field

[a]alberto.boaron@unige.ch

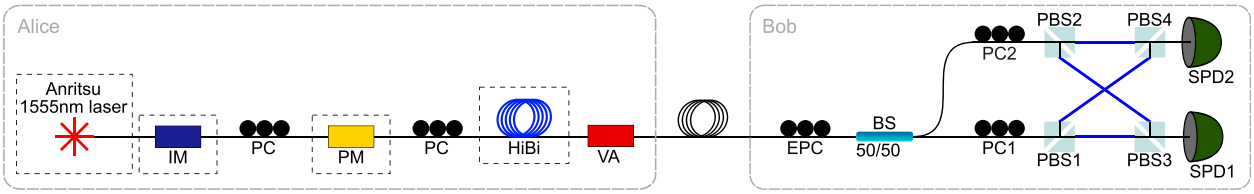

FIG. 1. Schematics of the experimental setup. IM, intensity modulator; PC, polarization controller; PM, phase modulator based on a lithium niobate waveguide; HiBi, high birefringence fiber; VA, variable attenuator; PBS, polarizing beamsplitter; BS, beamsplitter; EPC, electronic polarization controller; and SDP, single-photon detector. The arm connecting the BS and the PC2 introduces a delay of 800 ps compared to the arm from the BS to the PC1 due to a difference in length. The blue lines connecting the PBS are polarization-maintaining fiber and have the same length. The dashed lines denote temperature stabilized boxes.

programmable gate arrays (FPGAs) placed on Alice's and Bob's side. On Alice's side, a gain-switched DFB laser at 1554.94 nm [Anritsu], triggered at 625 MHz, generates phase-randomized weak coherent pulses with a pulse duration of 93 ps. An intensity modulator [Photline] based on an integrated Mach-Zehnder interferometer on lithium-niobate ($LiNbO_3$) then encodes the decoy levels. The polarization encoding is done by a titanium indiffused $LiNbO_3$ phase modulator (PM) [Thorlabs]. The pulses are injected in it with a polarization $(|H\rangle + |V\rangle)/\sqrt{2}$. We control the relative phase ϕ between $|H\rangle$ and $|V\rangle$ by applying a voltage on the PM to change its birefringence. At the output, we then have the state $(|H\rangle + e^{i\phi}|V\rangle)/\sqrt{2}$. The phase $\phi \in \{0, \pi/2, \pi\}$ is randomly chosen by the FPGA and set by a 3-level digital-to-analog converter made in-house. The PM introduces a polarization mode delay of 10.7 ps that is compensated by 8 m of high birefringence (HiBi) fiber. Alice chooses the basis X with a probability $p_X^A = \frac{1}{8}$. At the output of Alice's device, an attenuator sets the correct mean photon number of the outgoing pulses.

Bob's basis choice is made by a symmetric beamsplitter (BS), meaning that $p_Z^B = p_X^B = \frac{1}{2}$. The splitting ratio could be optimized for each distance. However, for short distances, $p_Z^B > \frac{1}{2}$ is not advantageous since the detectors are saturated, and for longer distances, p_X^B has to be increased to have enough statistics in the X basis. So, for simplicity, we chose a 50:50 splitting ratio as a good compromise for almost all distances. Two polarization controllers, PC1 and PC2, are set such that the two fiber-based polarizing beamsplitters, PBS1 and PBS2 (extinction ratios >20 dB), perform a projection in the Z (rectilinear) and X (diagonal) bases, respectively. The output ports corresponding to $|H\rangle$ and $|V\rangle$ are recombined with $|+\rangle$ and $|-\rangle$ via two other PBSs. To distinguish between the two bases, an additional delay of 800 ps is introduced in the arm of the X basis. With this temporal multiplexing, we are able to use only two detectors instead of four. We employ in-house made free-running single-photon detectors based on InGaAs/InP negative feedback avalanche photodiodes cooled by a free-piston Stirling cooler to achieve dark count rates of 10 Hz.[21] Note that for shorter distances up to 100 km, it would be more appropriate to use four detectors in order to reduce the saturation. Moreover, Peltier cooling would be sufficient, as dark counts are less critical.

The polarization of the pulses during transmission is prone to fluctuations, e.g., due to temperature drifts. To compensate for these fluctuations, we have implemented a feedback loop based on the trial-and-error approach that acts on an electronic polarization controller (EPC) [Phoenix Photonics] placed at the input of Bob's setup. This EPC is composed of three adjustable phase plates based on small HiBi fiber pieces whose temperature is adjusted to change their birefringence. The third one is set such that it affects only the phase between $|H\rangle$ and $|V\rangle$ and by consequence the quantum bit error rate (QBER) in the X basis. Thus, the feedback loop takes the QBER in the Z basis as the error signal to control the first two wave-plates and in the X basis for the third one. Note that the QBER in the X basis is directly given by the probability to detect the state $|-\rangle$ when the basis X is prepared. In the Z basis, the QBER Q_Z is provided in real-time by the Cascade error correction algorithm. This approach exempts us to use additional lasers to monitor the polarization drifts.[22]

We perform exchanges of secret keys with complete distillation, i.e., taking into account the finite statistics effect for the privacy amplification, for different transmission distances. The quantum channel is composed of a fiber spool of 12 km and a variable attenuator set to a value η_{att} to simulate additional optical fiber with a loss of 0.2 dB/km. In order to test the polarization stabilization scheme, we also perform a key exchange with more than 100 km of real fiber. For all measurements, the sizes of the error correction blocks and the privacy amplification blocks are set to $n_Z^{EC} = 8192$ and $n_Z = 8.192 \times 10^6$, respectively. These parameters offer a good compromise between the time of acquisition and the effect of finite-key statistics on the secret kay rate (SKR). The security parameters are fixed to $\epsilon_{sec} = 10^{-9}$ and $\epsilon_{corr} = 10^{-15}$.

For every result depicted in Fig. 2, the SKR has been maximized by optimizing the mean photon numbers μ_1 and μ_2, the probability p_{μ_1}, and the detector parameters, i.e.,

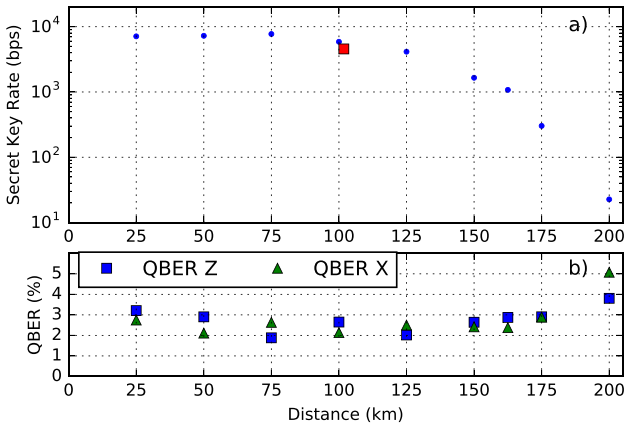

FIG. 2. SKR (a) and QBER (b) as a function of the transmission distance. The measurements were done using a quantum channel composed of 12.16 km of real fiber and attenuation to simulate additional distances. The red square indicates a measurement done with more than 100 km of real fiber.

temperature, dead-time, and efficiency. The QBER due to polarization misalignment is automatically minimized via the feedback that acts on the EPC.

From Fig. 2, we can clearly identify three regimes. Up to 125 km, the SKR is mainly limited by the saturation of the detectors due to a dead-time around 30 μs. Therefore, it is favourable to keep the mean photon number of the states sent by Alice low. At 25 km, we use $\mu_1 = 0.10$, $\mu_2 = 0.06$, and $p_{\mu_1} = 0.56$. In this range, the SKR could be improved by employing faster single-photon detectors such as superconducting nanowire single-photon detectors[23] or gated avalanche photodiodes.[24] Nevertheless, the InGaAs single-photon detectors we use are much less complex. Above 125 km, the SKR decreases exponentially as expected due to the fiber loss, until around 175 km where the dark-count rate becomes significant compared to the detection rate and, as a consequence, the QBER increases rapidly. At this distance, the settings are $\mu_1 = 0.33$, $\mu_2 = 0.14$, and $p_{\mu_1} = 0.75$. We achieve a SKR of 303 bps. This result is comparable to other state of the art of long-distance QKD experiments.[23,25–27] Moreover, the SKRs are better than other two-decoy/four-state BB84 experiments.[11,28] Indeed, our simulations show that up to about 175 km, the one-decoy level approach is slightly more efficient than the two-decoy one. Finally, the SKR at 200 km is 23 bps.

To conclude, we implemented a BB84 protocol with states encoded in the polarization DoF of weak coherent pulses. Our source is based on only one pulsed laser in order to prevent side-channel attacks. It could be used for both fiber and free space implementations. We kept the system simple with a three-state encoding approach with only one decoy-state level. Therefore, we have in total 6 different states instead of 12 for the complete protocol, which greatly simplifies the state preparation and the data processing. Using a rigorous security analysis taking into account finite-key effects, we distilled secret keys at a rate of 23 bps for a distance of 200 km.

We would like to acknowledge Jesús Martínez-Mateo for providing the error correction code, Gianluca Boso for his contribution in building the control electronics, Raphael Houlmann for the FPGA programming, and Charles Ci Wen Lim for the useful discussions about the security proof. We thank the Swiss NCCR QSIT and Davide Rusca thanks the EUs H2020 programme under the Marie Skłodowska-Curie Project QCALL (GA 675662) for financial support.

[1]H.-K. Lo, M. Curty, and K. Tamaki, Nat. Photonics **8**, 595 (2014).
[2]C. H. Bennett and G. Brassard, in *International Conference on Computers, Systems & Signal Processing*, Bangalore, India, 9–12 December 1984, pp. 175–179.
[3]A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[4]C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[5]F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[6]K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002).
[7]D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, Appl. Phys. Lett. **87**, 194108 (2005).
[8]T. Sasaki, Y. Yamamoto, and M. Koashi, Nature **509**, 475 (2014).
[9]J. C. Bienfang, A. J. Gross, A. Mink, B. J. Hershman, A. Nakassis, X. Tang, R. Lu, D. H. Su, C. W. Clark, C. J. Williams, E. W. Hagley, and J. Wen, Opt. Express **12**, 2011 (2004).
[10]X. Tang, L. Ma, A. Mink, A. Nakassis, H. Xu, B. Hershman, J. C. Bienfang, D. Su, R. F. Boisvert, C. W. Clark, and C. J. Williams, Opt. Express **14**, 2062 (2006).
[11]Y. Liu, T.-Y. Chen, J.-H. J. Wang, W.-Q. Cai, X. Wan, L.-K. Chen, S.-B. Liu, H. Liang, L. Yang, C.-Z. Peng, K. Chen, Z.-B. Chen, and J.-W. Pan, Opt. Express **18**, 8587 (2010).
[12]S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, Nature **549**, 43 (2017).
[13]S. Nauerth, M. Fürst, T. Schmitt-Manderbach, H. Weier, and H. Weinfurter, New J. Phys. **11**, 065001 (2009).
[14]A. Huang, S.-H. Sun, Z. Liu, and V. Makarov, preprint arXiv:1711.00597 (2017).
[15]A. Boaron, B. Korzh, R. Houlmann, G. Boso, C. C. W. Lim, A. Martin, and H. Zbinden, J. Appl. Phys. **120**, 063101 (2016).
[16]X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).
[17]C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, Phys. Rev. A **89**, 022307 (2014).
[18]J. Martinez-Mateo, C. Pacher, M. Peev, A. Ciurana, and V. Martin, Quantum Inf. Comput. **15**, 453 (2015), see http://dl.acm.org/citation.cfm?id=2871401.2871407.
[19]C. Bennett, G. Brassard, C. Crepeau, and U. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).
[20]D. Rusca, A. Boaron, F. Grünenfelder, A. Martin, and H. Zbinden, preprint arXiv:1801.03443 (2018).
[21]B. Korzh, N. Walenta, T. Lunghi, N. Gisin, and H. Zbinden, Appl. Phys. Lett. **104**, 081108 (2014).
[22]G. B. Xavier, G. Vilela de Faria, G. P. Temporão, and J. P. von der Weid, Opt. Express **16**, 1867 (2008).
[23]S. Wang, W. Chen, J.-F. Guo, Z.-Q. Yin, H.-W. Li, Z. Zhou, G.-C. Guo, and Z.-F. Han, Opt. Lett. **37**, 1008 (2012).
[24]L. C. Comandar, B. Fröhlich, M. Lucamarini, K. A. Patel, A. W. Sharpe, J. F. Dynes, Z. L. Yuan, R. V. Penty, and A. J. Shields, Appl. Phys. Lett. **104**, 021101 (2014).
[25]H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, Nat. Photonics **1**, 343 (2007).
[26]D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, New J. Phys. **11**, 075003 (2009).
[27]B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, Nat. Photonics **9**, 163 (2015).
[28]B. Fröhlich, M. Lucamarini, J. F. Dynes, L. C. Comandar, W. W.-S. Tam, A. Plews, A. W. Sharpe, Z. Yuan, and A. J. Shields, Optica **4**, 163 (2017).