Cryptographic security concerns on timestamp sharing via a public channel in quantum-key-distribution systems

Melis Pahalı [*] and Kadir Durak [†]
Electrical and Electronics Engineering Department, Özyeğin University, Istanbul 34794, Turkey

Utku Tefek [‡]
Advanced Digital Sciences Center, Singapore 138602, Singapore

(Received 8 March 2022; accepted 11 July 2022; published 26 July 2022)

Quantum-key-distribution protocols are known to be vulnerable against a side channel attack that exploits the time difference in detectors' responses used to obtain key bits. The recommended solution against this timing side channel attack is to use a large time bin width instead of high-resolution timing information. A common notion is that using a large bin width reduces the resolution of detectors' responses, hence supposedly minimizes the information leakage to an eavesdropper. We challenge this conventional wisdom and demonstrate that increasing the bin width does not monotonically reduce the mutual information between the key bits and the eavesdropper's observation of detectors' responses. Instead of randomly increasing the bin width, it should be carefully chosen because the mutual information fluctuates with respect to the bin width. We also examine the effect of full width half maximums (FWHMs) of the detectors' responses on the mutual information and show that decreasing the FWHM increases the mutual information. Lastly, the start time of binning is also shown to be important in the binning process and the mutual information fluctuates periodically with respect to it.

DOI: 10.1103/PhysRevA.106.012611

I. INTRODUCTION

The general scheme of quantum-key-distribution (QKD) protocols [1,2] is well known; their security proofs [3–7], side channels of QKD systems [8–14], and side channel attacks [15–25] are widely studied topics. In this paper, we study the timing side channel, which can also be referred to as the detector efficiency mismatch [8,15,24].

Before starting a QKD protocol, detection modules need to be characterized. The characterization involves time synchronization between authorized communicating parties. Time synchronization involves determining the path differences between different receivers to the transmitter, and then compensating these path differences physically or digitally (as a postprocess). Path differences in a QKD experimental setup are represented in terms of time differences between detectors' responses. During QKD, two communicating parties share the basis set in which a photon detection is realized and the timestamp of this event via a classical channel to determine the coincidences, to generate raw key bits, and to compute the quantum bit error rate and/or the amount of violation of Bell's inequality depending on the protocol that is followed. The timestamps of the events are important in order to determine the coincidences correctly. When the time synchronization is not perfect but realized up to a precision, the coincidences can still be determined correctly; however, a timing side channel attack can occur within that precision. An eavesdropper can estimate the raw key bits, which are required to be kept secret, by simply observing the timestamps and the relative delay between coincidence events in the same basis set. In other words, nonoverlapping coincidences in the time domain make the values of raw key bits predictable for the eavesdropper. In summary, the timing side channel can be understood as the exploitable correlation between the timestamps and the measurement results obtained from the quantum channel. Measurement results carry the bit content and therefore the security relies on them.

In the literature, the recognized solution to this problem is to minimize the eavesdropper's information by increasing the time bin width for the publicly shared detection times [26]. And only two values of time bin width are examined. However, in this study, we examine a range of bin width values and show that arbitrarily increasing the bin width does not necessarily mitigate timing side channel attacks. Instead, the bin width should be carefully chosen depending on the delay between the coincidences.

In this paper, we analyze the timing side channel of a QKD system with imperfect time synchronization such that the delays in coincidences are caused by the imperfect synchronization, but not caused by clock drifts.

The paper is organized as follows: a detailed analysis of the mutual information is discussed in Sec. II; two important parameters in the mutual information, i.e., the start time of binning and the full width half maximum (FWHM) of the detector response, are discussed in Secs. III and IV, respectively; and important findings are summarized in Sec. V.

[*] melis.pahali@ozu.edu.tr
[†] kadir.durak@ozyegin.edu.tr
[‡] u.tefek@adsc-create.edu.sg

II. MUTUAL INFORMATION

In an entanglement-based QKD system, two communicating parties Alice and Bob measure incoming photons in their detection modules to obtain raw key bits. A detection module involves a number of noncommuting basis sets. A property represented by a discrete variable of the incoming photon is measured in one of the noncommuting basis sets. For example, the polarization of a photon is measured in one of the detector sets dedicated to (0°, 90°) and (−45°, 45°) polarization measurements and a bit is obtained. To note that, (0°, 90°) constitutes a basis set and each of the two orientations, 0° and 90°, carries a bit content. If entangled photon pairs traveling to Alice's and Bob's detection modules are measured in the same basis set, the measurement outcomes are used as raw key bits. For each pair of bits, it is considered whether they are raw key bits, violation of Bell's inequality bits, or discarded bits according to the coincided basis sets among the communicating parties. Similarly, in a prepare and measure (PaM) QKD system, the scenario is similar but the measurement outcomes obtained from all the basis sets are used as raw key bits as long as Alice's and Bob's basis sets are matching. Again, the measurement basis sets or bases and timestamps are publicly shared in these systems, which makes PaM protocols also vulnerable against timing side channel attacks. This is because any time difference between coincidences obtained from the same basis sets makes those bit contents distinguishable. For the clarity of content, we will continue with the entanglement-based QKD protocol. However, the calculations are valid and can be repeated for PaM protocols also.

In QKD protocols, single-photon avalanche diodes (SPADs) are commonly used for the detection of photons. For an incident photon, a SPAD outputs a transistor-transistor logic (TTL) signal to create a register having the detection time. There is a time difference between the time that the photons falls onto the active area of the SPAD and the generation of a TTL signal. This time difference is a distribution rather than a constant value. This timing histogram is called timing jitter or, simply, detector response. As the model of a detector response, we work with Eq. (1) [26], which is an exponentially modified Gaussian distribution

$$d(t) = \frac{1}{2\tau_e} e^{-\frac{\tau_G}{4\tau_e^2}} \cdot e^{\frac{t-t_0}{\tau_e}} \operatorname{erfc}\left(\frac{t-t_0}{\tau_G}\right), \tag{1}$$

where "·" is the convolution product, τ_e and τ_G are model parameters, and the peak density of $d(t)$ is observed at $t = t_0$. The values for a reference detector are $\tau_e = 400$ ps, $\tau_G = 290$ ps, and $t_0 = 1000$ ps. A second detector also has the same parameters, except for t_0. By changing the value of t_0 for the second detector, a Δt_0 time difference between the two detectors is generated. The profile of the reference detector is the blue (continuous) curve in Fig. 1. In Fig. 1, the y axis represents the normalized frequency of occurrence, which is equivalent to the probability density for the original timing histogram.

Since there are two detectors dedicated to the measurement of raw key bits in one basis set, there are also two different paths a photon can traverse. Each path contains an optical path plus a distance from the start to the peak position of the detector response. In the most general case, Δt_0 is the timing difference between two detectors due to optical path distances and electrical delays. But in Fig. 2(a), it is shown as only an extra optical path for visualization. For example, if the raw key bit detection parts of the detection modules at Alice's and Bob's sides are represented schematically as in Fig. 2(a), the photon that goes to D_+ travels more than the one that goes to D_-. If the entangled state in the quantum channel between Alice and Bob is $(|00\rangle + |11\rangle)/\sqrt{2}$, then the coincidence events coming from the detectors D_+ and D'_+, and D_- and D'_-, are seen as separate peaks in a cross-correlogram, as shown in the sketch in Fig. 2(b). The existence of this time difference will cause information leakage to an eavesdropper. This information leakage is quantified with mutual information which is a measure of the eavesdropper's information gain about the key bit value [27,28].

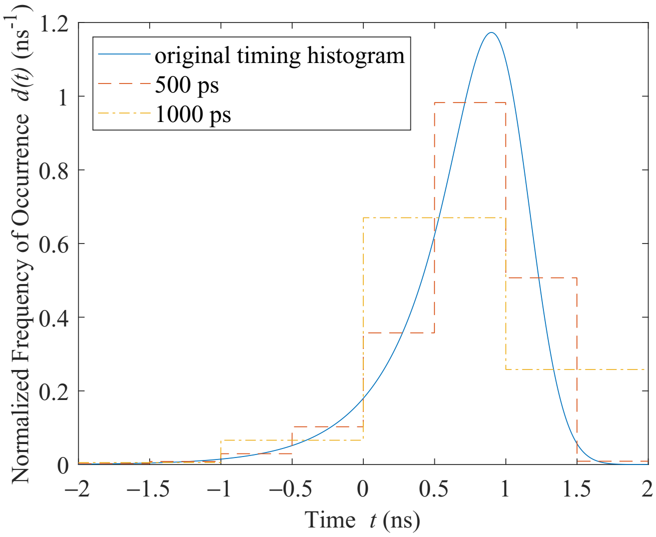
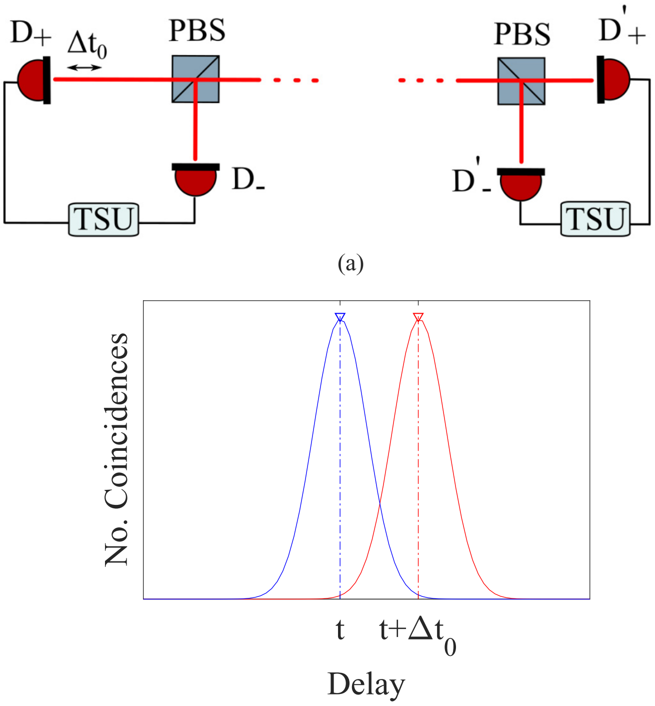


FIG. 1. The graph of the normalized frequency of occurrence dependence to time. Blue (continuous) curve is the original timing histogram of the detector, red (dashed) and yellow (dot-dashed) curves are the binned versions of the original histogram, and the legend represents bin width values.

Time bin is the unit time interval used in a QKD system. In every time bin, a measurement may be performed in detection modules, and if there is a measurement, one bit of information contributing to a bit string may be obtained. The time bin width determines the precision of the timing histograms and the precision of the timestamp information revealed via the classical channel by the communicating parties. However, there are processes which are binning for discrete time signals and quantization for continuous time signals. In the binning process, the value of the bin width is redetermined and representative values for the normalized frequency of occurrences falling into each time bin are regenerated. In our study, we work with discrete time signals, namely, quantized continuous time signals, and we apply the binning process to them. As an example of the binning process, in Fig. 1, the red (dashed) and yellow (dot-dashed) curves are the binned versions of the original timing histogram. The bin width is 500 ps in the red (dashed) curve and 1000 ps in the yellow (dot-dashed) curve.

In the literature, it is known that the binning process with a large bin width value reduces the mutual information; how-



(a)

(b)

FIG. 2. (a) Schematic representation of the detectors in the same basis sets at Alice's (left) and Bob's (right) sides. PBS: polarizing beam splitter. D_+ (D'_+) and D_- (D'_-) are detectors in the transmitted and reflected outputs, respectively. TSU: timestamp unit. Δt_0 is an extra optical path. (b) The cross-correlogram of coincidence events between Alice and Bob. t is the time difference between D_- and D'_-, and $t + \Delta t_0$ is the time difference between D_+ and D'_+. Since there is an extra optical path, there are two separate peaks in the cross-correlogram.

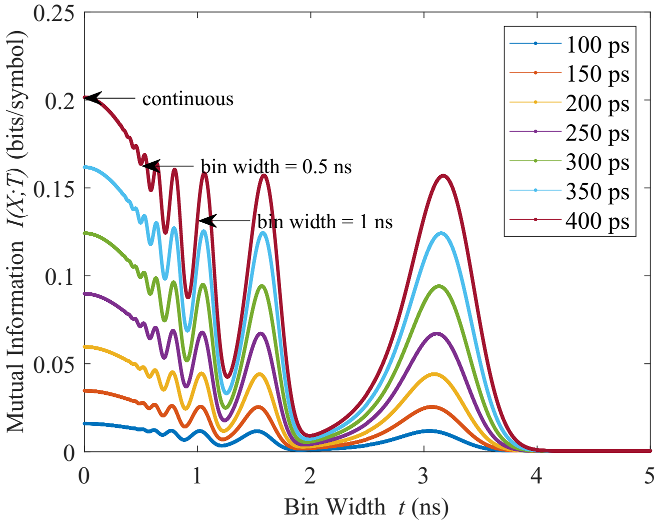


FIG. 3. The graph of the mutual information dependence to the bin width and Δt_0. The legend represents Δt_0 values. The curves, from bottom to top, correspond to Δt_0 from 100 ps to 400 ps.

ever, in this study, we show that not every increment of the value of the bin width gives a reduction in the mutual information. Instead, there is a fluctuation behavior, which is explained in the rest of the paper.

The mutual information $I(X;T)$ between the raw key bit values and detection times can be expressed as in Eq. (2),

$$
\begin{aligned}
I(X;T) &= \sum_x \int p(x,t)\log_2\left[\frac{p(x,t)}{p(x)p(t)}\right]dt \\
&= \sum_x \int p(x)p(t|x)\log_2\left[\frac{p(t \mid x)}{p(t)}\right]dt \\
&= \sum_x \int p^0(x)d_x(t)\log_2\left[\frac{d_x(t)}{\bar{d}(t)}\right]dt \\
&= \sum_x p^0(x)\int d_x(t)\log_2 d_x(t)dt \\
&\quad - \int \bar{d}(t)\log_2\bar{d}(t)dt,
\end{aligned}
\tag{2}
$$

where the first line follows from the definition of mutual information and the third from substituting the relevant distributions. Namely, $p^0(x)$ is the probability mass function of the symmetric Bernoulli random variable x. $d_x(t)$ is the probability density of taking a click at time t, given x. For example, $d_0(t)$ is the probability of taking a click for 0 at time t. Therefore, $d_0(t)$ and $d_1(t)$ are the detectors' responses of the detectors dedicated to obtaining 0 and 1, respectively. $d_0(t)$ and $d_1(t)$ differ by Δt_0 as described above. Namely, while the peak density of $d_0(t)$ is positioned at t_0, the peak density of $d_1(t)$ is positioned at $t_0 + \Delta t_0$. $\bar{d}(t)$ is the probability density of taking a click at time t from an ensemble of detectors. The last step follows from algebraic manipulations and substituting Eq. (3),

$$
\bar{d}(t) = \sum_x p^0(x)d_x(t). \tag{3}
$$

Mutual information is computed for various Δt_0 values and it fluctuates as shown in Fig. 3 with varying bin width values. For each bin width value, binning is started at the same point of the original timing histogram so there is no phase difference between the binning processes. Bin widths of 0.5 ns and 1 ns as the evaluation points on the continuous time signal in [26] are shown on the $\Delta t_0 = 400$ ps (upper most) curve in Fig. 3 for comparison. The fluctuating behavior of the mutual information with increasing bin width indicates that a combination of bin width and Δt_0 should be chosen carefully to minimize the mutual information.

III. START TIME OF BINNING

The index of the time bin at which a photon detection event is registered depends on the start time of binning as well as the bin width. Mutual information changes according to the start time of binning; it is periodic with respect to it for a constant bin width value and the period is equal to the bin width itself. As a result, the start time of binning is also very critical for QKD security. In order to model this behavior, we use a Gaussian distribution for timing histograms of two detectors from now on. For illustrating the effect of the start time of binning on the mutual information, we considered the following values: Δt_0 is taken as 350 ps, the FWHMs

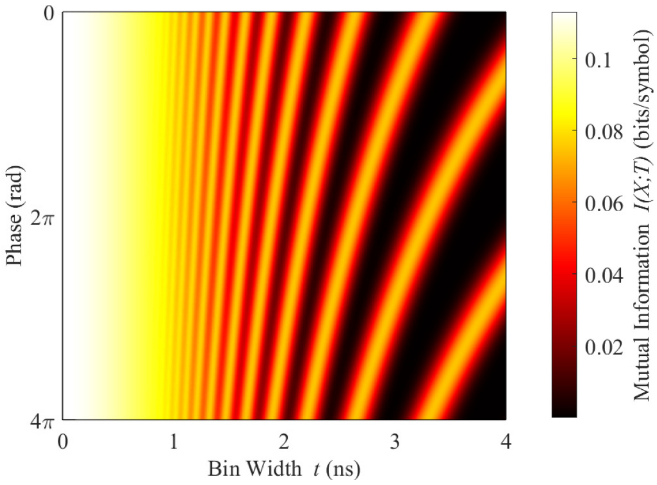


FIG. 4. The graph of the mutual information dependence to the start time of binning. The start time of binning is represented in terms of phase. The color bar represents the mutual information.

of the detectors' responses are taken as 1 ns, and the mutual information is calculated for bin width values ranging from 0 to 4 ns in Fig. 4. In all the mutual information calculations related to different values of the bin width, the phase at the start is 0 and, after one bin width, the phase becomes 2π. Instead of showing the start time of binning as an axis in Fig. 4, we chose the phase as a better indicator of periodicity. In order to clearly show the periodicity, the phase is chosen from 0 to 4π. This graph shows that even a carefully chosen bin width is not sufficient for QKD security as the start timing of binning also plays a crucial role.

IV. FWHM OF DETECTOR RESPONSE

In the QKD market, there is a variety of companies offering detectors having low time jitters, which are characterized by FWHMs, as products in order to allow high key rates in QKD implementations. On the other hand, for a constant Δt_0, when the FWHMs of the detectors' responses decrease, the overlap portion of their timing histograms decreases and their profiles become distinguishable, as can be seen in Fig. 5, and ultimately the mutual information increases. For this reason, detectors having low time jitters are vulnerable to the timing side channel attack.

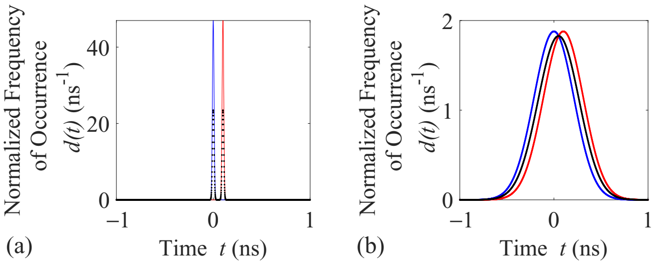


FIG. 5. The effect of the FWHMs of detectors' responses having $\Delta t_0 = 100$ ps on the distinguishability of the profiles and hence the values of coincidences. Blue (dark gray) and red (light gray) curves are two detectors' responses. The black curve is the summation of them after they are multiplied by 0.5. The distinguishability of the two can be seen in the summation curve. (a) FWHMs = 20 ps. (b) FWHMs = 500 ps.

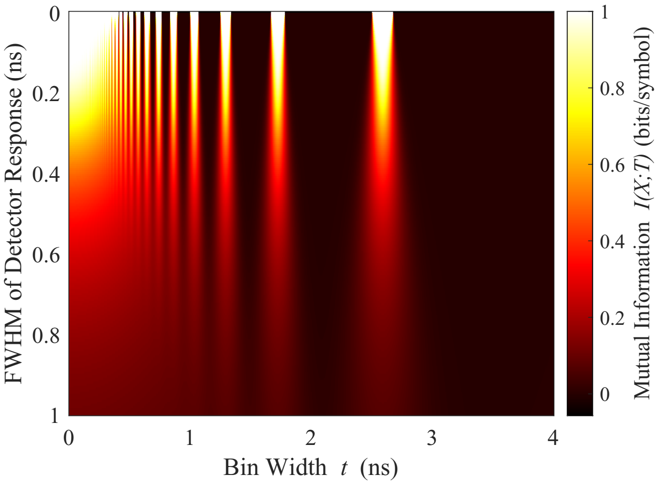


FIG. 6. The graph of the mutual information dependence to the FWHMs of detectors' responses with varying bin width. The color bar represents the mutual information.

Figure 6 shows the scan of the FWHM of the detector response and bin width values for $\Delta t_0 = 350$ ps. A constant start time of binning is used for varying bin widths. It is very critical that when the FWHM of the detector response is smaller than Δt_0, the mutual information is almost 1. This is a direct consequence of the fact that the coincidence peaks in the cross-correlogram are almost completely distinguishable from the publicly shared timestamps and basis sets when the FWHM of the detector response is smaller than Δt_0. The message that should be taken from this graph is that the FWHMs of the detectors' responses should be negligible compared to Δt_0. More generally, the coincidence peaks in the cross-correlogram should overlap as much as possible. This can easily be arranged in a typical QKD setup by a careful physical adjustment of the distances from the PBS to the detectors, and using the detectors with the same (or similar) FWHMs of the responses and/or electronic delays. However, an exhaustive search of ways to externally give a delay to one of the coincidence curves is required to prevent a loophole in the security of the QKD system.

The timing side channel mentioned in this work is due to the timestamp and basis set information sharing of Alice and Bob in the public channel. An alternative solution to this problem is that only Alice (Bob) shares the timestamp and basis set information in the public channel and Bob (Alice) checks for the distinguishability in the cross-correlogram peaks of the + and − coincidences. After the analysis, Bob eliminates the offset delay in one of the detectors to make the cross-correlogram peaks completely overlapping. After this compensation, Bob can share his timestamp and basis set information with Alice in the public channel. In this way, the eavesdropper never learns about the relative delay in coincidences from different detector sets in a basis set. Also, measurement-device-independent schemes can be applied to eliminate this problem.

V. CONCLUSION

As a conclusion, in order to reduce or minimize the information leakage to an eavesdropper, choosing the bin width and start time of binning values is very important in QKD protocols because the mutual information fluctuates with respect to the bin width and the mutual information periodically fluctuates with respect to the start time of binning. Therefore, it can be concluded that arbitrarily increasing the bin width is not a precaution to a timing side channel attack. For the security of a QKD system, the bin width, the start time of binning and the ratio of the FWHMs of the detectors' responses to the time difference between the timing histograms or the coincidence peaks in the cross-correlogram should be carefully adjusted with the characterization of physical system parameters. It is also possible to avoid the timing side channels by allowing one side to compensate for the time delays between cross-correlogram peaks.

ACKNOWLEDGMENT

This research was supported by the Scientific and Technological Research Council of Turkey (TÜBİTAK), Academic Research Funding Programs Directorate (ARDEB), Primary Subjects R&D Funding Program (Program No. 1003), Project No. 118E991.

[1] Ekert, Quantum Cryptography Based on Bell's Theorem, Phys. Rev. Lett. **67**, 661 (1991).

[2] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, Theor. Comput. Sci. **560**, 7 (2014).

[3] R. Renner, Security of quantum key distribution, Intl. J. Quantum Inf. **06**, 1 (2008).

[4] C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma, Security proof of quantum key distribution with detection efficiency mismatch, Quantum Inf. Comput. **9**, 131 (2009).

[5] Y. Zhang, P. J. Coles, A. Winick, J. Lin, and N. Lütkenhaus, Security proof of practical quantum key distribution with detection-efficiency mismatch, Phys. Rev. Research **3**, 013076 (2021).

[6] M. Curty, K. Azuma, and H.-K. Lo, Simple security proof of twin-field type quantum key distribution protocol, npj Quantum Inf. **5**, 64 (2019).

[7] E. Biham, M. Boyer, P. Boykin, T. Mor, and V. Roychowdhury, A proof of the security of quantum key distribution, J. Cryptology **19**, 381 (2006).

[8] V. Makarov, A. Anisimov, and J. Skaar, Effects of detector efficiency mismatch on security of quantum cryptosystems, Phys. Rev. A **74**, 022313 (2005).

[9] C.-H. F. Fung, B. Qi, K. Tamaki, and H.-K. Lo, Phase-remapping attack in practical quantum-key-distribution systems, Phys. Rev. A **75**, 032314 (2007).

[10] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Thermal blinding of gated detectors in quantum cryptography, Opt. Express **18**, 27938 (2010).

[11] B. Mao, W. Hu, A. Althoff, J. Matai, J. Oberg, D. Mu, T. Sherwood, and R. Kastner, Quantifying timing-based information flow in cryptographic hardware, in *Proceedings of the IEEE/ACM International Conference on Computer-Aided Design*, ICCAD '15 (IEEE Press, Washington, USA, 2015) p. 552–559.

[12] B. Mao, W. Hu, A. Althoff, J. Matai, Y. Tai, D. Mu, T. Sherwood, and R. Kastner, Quantitative analysis of timing channel security in cryptographic hardware design, IEEE Trans. Comput.-Aid. Des. Integr. Circuits Syst. **37**, 1719 (2018).

[13] A. K. Biswas, A. Banerji, P. Chandravanshi, R. Kumar, and R. P. Singh, Experimental side channel analysis of bb84 qkd source, IEEE J. Quantum Electron. **57**, 1 (2021).

[14] A. Duplinskiy and D. Sych, Bounding passive light-source side channels in quantum key distribution via Hong-Ou-Mandel interference, Phys. Rev. A **104**, 012601 (2021).

[15] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems, Phys. Rev. A **78**, 042333 (2008).

[16] F. Xu, B. Qi, and H. Lo, Experimental demonstration of phase-remapping attack in a practical quantum key distribution system, New J. Phys. **12**, 113026 (2010).

[17] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, Nat. Photon. **4**, 686 (2010).

[18] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Full-field implementation of a perfect eavesdropper on a quantum cryptography system, Nat. Commun. **2**, 349 (2011).

[19] L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar, and V. Makarov, Controlling a superconducting nanowire single-photon detector using tailored bright illumination, New J. Phys. **13**, 113042 (2011).

[20] V. Makarov and D. Hjelme, Faked states attack on quantum cryptosystems, J. Mod. Opt. **52**, 691 (2005).

[21] A. Vakhitov, V. Makarov, and D. Hjelme, Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography, J. Mod. Opt. **48**, 2023 (2001).

[22] Y.-L. Tang, H.-L. Yin, X. Ma, C.-H. F. Fung, Y. Liu, H.-L. Yong, T.-Y. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, Source attack of decoy-state quantum key distribution using phase information, Phys. Rev. A **88**, 022308 (2013).

[23] H. Weier, H. Krauss, M. Rau, M. Fuerst, S. Nauerth, and H. Weinfurter, Quantum eavesdropping without interception: An attack exploiting the dead time of single-photon detectors, New J. Phys. **13**, 073024 (2011).

[24] B. Qi, C. Fung, H. Lo, and X. Ma, Time-shift attack in practical quantum cryptosystems, Quantum Inf. Comput. **7**, 73 (2007).

[25] J. Yin, Y.-H. Li, S. Liao, M. Yang, Y. Cao, L. Zhang, J.-G. Ren, W. Cai, W. Liu, S.-L. Li, R. Shu, Y. Huang, L. Deng, L. Li, Q. Zhang, N. Liu, Y. Chen, C.-Y. Lu, X. bin Wang, F. Xu *et al.*,

Entanglement-based secure quantum cryptography over 1120 kilometres, Nature (London) **582**, 501 (2020).

[26] A. Lamas-Linares and C. Kurtsiefer, Breaking a quantum key distribution system through a timing side channel, Opt. Express **15**, 9388 (2007).

[27] D. Bruss, Optimal Eavesdropping in Quantum Cryptography with Six States, Phys. Rev. Lett. **81**, 3018 (1998).

[28] A. Rastegin, On conclusive eavesdropping and measures of mutual information in quantum key distribution, Quantum Inf. Proc. **15**, 1225 (2016).