
Article:
Taylor, Ben J., Smith, Peter R., Dynes, James F. et al. (2026) Practical Countermeasure Against Attacks Exploiting Detection Efficiency Mismatch in Quantum Key Distribution. Physical Review Applied. 054029. ISSN: 2331-7019

https://doi.org/10.1103/7zhl-5vv1

Practical countermeasure against attacks exploiting detection-efficiency mismatch in quantum key distribution

Ben J. Taylor,[1,2,*] Peter R. Smith,[1] James F. Dynes,[1] Robert I. Woodward,[1] Marco Lucamarini,[2] R. Mark Stevenson,[1] and Andrew J. Shields[1]

[1] *Toshiba Europe Limited, 208 Cambridge Science Park, Cambridge CB4 0GZ, United Kingdom*

[2] *School of Physics, Engineering & Technology and York Centre for Quantum Technologies, University of York, York YO10 5FT, United Kingdom*

(Received 30 December 2025; revised 17 February 2026; accepted 26 March 2026; published 12 May 2026)

We demonstrate a practical countermeasure against a well-known class of attacks on quantum key distribution (QKD) systems that exploit detection-efficiency mismatch, where the receiver's detectors do not exhibit identical responses to incoming photons across all degrees of freedom. This class of quantum hacking strategies is broad and significantly includes the time-shift attack, which targets an arrival-time-dependent side-channel at the receiver. The four-state countermeasure, previously only proven to be secure in theory, is implemented here on a gigahertz-clocked prototype QKD system and evaluated for its security and performance. We show that its presence enables almost complete recovery of the system's ideal secret key rate. Our results provide strong justification for adopting this countermeasure as a standard component in future scalable and practical QKD systems.

DOI: 10.1103/7zhl-5vv1

I. INTRODUCTION

Quantum key distribution (QKD) offers unconditionally secure communication guaranteed by the laws of quantum mechanics, provided that the protocol's physical implementation does not deviate from its theoretical description. As QKD technology has matured and progressed towards standardized real-world deployment [1,2], the field of implementation security, where security can be proven even with known hardware imperfections [3], plays an increasingly vital role.

One approach to achieving this adapts security proofs to capture the impacts of imperfections, according to experimental characterization. Alternatively, *countermeasures* can be introduced in hardware or software, defined as modifications that close certain attack vectors or reduce side-channel information leakage to a potential eavesdropper (Eve). These countermeasures typically still require their own characterizations, for example, bounding photon statistics of weak coherent pulses for implementing the decoy-state method [4,5]. Protocols such as measurement-device-independent [6,7] or twin-field QKD [8] grant adversaries full control over the detection system, but must deal with hardware imperfections at the transmitter. Full device-independence in QKD remains extremely challenging in practice with current technology [9].

In prepare-and-measure schemes such as BB84 [10], the receiver is considered the most vulnerable element, as it necessarily accepts all light from the insecure quantum channel. Consequently, it has been the primary target of quantum hacking attempts, such as blinding [11–13], faked-state [14,15], and Trojan horse [16,17] attacks.

The specific receiver imperfection considered in this paper is the mismatch in detection efficiency between two single-photon detectors, a side-channel commonly exploited in the quantum hacking literature, most notably and successfully via the time-shift attack [18,19] or in combination with a faked-state attack [20].

Here we investigate the performance and security of the best known countermeasure against these attacks, which is applicable to any active detection setup. The countermeasure has previously been addressed theoretically in [19–21], but despite reported usage in systems in [22,23], no implementation has been experimentally characterized against an attack based on detection-efficiency mismatch, to the best of our knowledge. Our work therefore bridges an unresolved theory-experiment gap for high-speed QKD. This technique has been known by several names: *detector symmetrization* [24], *randomization* [25], *scrambling* [26], or *four-state Bob* [19,20]. The latter term is most descriptive of the hardware change made to the QKD receiver's

*Contact author: ben.taylor@toshiba.eu

phase modulator operation, so we adopt this terminology in our paper.

A. Detection-efficiency mismatch in QKD and the time-shift attack

Original security proofs assume that Bob's detectors, typically avalanche photodiodes (APDs) in modern commercial systems, exhibit identical photodetection responses across all degrees of freedom, including time, frequency, and polarization. This assumption implies perfectly matched detection efficiencies, η, and dark-count rates, regardless of the properties of the incident light or the electronic settings applied to each APD for a given operating condition. In practice, achieving such stringent uniformity is extremely challenging.

If this requirement is not met during a QKD system's operation, a bit-value-dependent (static) detection-efficiency mismatch will be present. This leads to a disparity in the number of 1s and 0s that form the raw, and eventually the sifted, keys, with no influence from Eve [27]. A significant deviation here would invalidate a critical cryptographic requirement of the final key's statistical randomness [28]. In this static mismatch case, with only a known difference between the APD 0 and APD 1 efficiencies, η_0 and η_1, to consider, security is recovered simply by amending the key generation rate by a prefactor [19]

$$\min\left(\frac{\eta_0}{\eta_0+\eta_1},\frac{\eta_1}{\eta_0+\eta_1}\right). \tag{1}$$

However, Eve is allowed to manipulate signals while in the quantum channel to affect the relative detection efficiency between Bob's APDs. By choosing an auxiliary degree of freedom to that of the encoding, she can gain significant knowledge of the key without increasing the quantum bit error rate (QBER) sufficiently to trigger Alice and Bob to abort their protocol. This was successfully demonstrated in the time-shift attack [18], which is the most technologically feasible strategy to exploit detection-efficiency mismatch in QKD.

A conceptual schematic of this attack is shown in Fig. 1. Eve controls a high-speed optical switch inserted into the channel, allowing her to choose between a shorter and longer optical path than the original fiber link, and so perturb the time-of-flight of each optical pulse passing through the channel. Using tunable optical delay lines and low-loss fiber [29], Eve can optimize these two time-shifts such that they correspond to the worst-case efficiency mismatches between Bob's APDs. These time-dependent mismatches may arise from different optical or electronic path lengths for signals going to each APD, or from inherent differences in the breakdown and threshold voltages of each semiconductor-based device [30]. APDs are typically gated with an electronic driving signal each clock cycle,

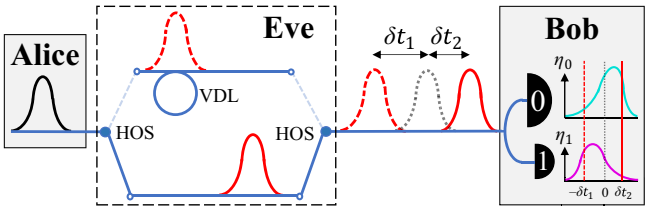

FIG. 1. Conceptual schematic of a time-shift attack. HOS, high-speed optical switch; VDL, variable optical delay line. Eve shifts optical pulses generated by Alice in time by $+\delta t_1$ or $-\delta t_2$, chosen to maximize mismatch on Bob's two nonidentical detectors, the efficiencies of which vary uniquely in time.

and each device will exhibit a unique time-dependent detection response across this gate.

When a significant mismatch is present, the probability that Bob detects a signal may depend as much on Eve's time-shift choice as the agreement between Alice and Bob's basis choice. While the key Alice and Bob output can still appear statistically random if Eve alternates time-shifts evenly, Eve will have greater knowledge than their privacy amplification has accounted for.

In the past two decades, several theoretical analyses have been presented that allow secure key rates in the presence of characterized detection mismatch [19,31–33]; a comprehensive summary of progress to date can be found in Table II of [34]. A significant practical weakness with this proof-based approach is that every possible auxiliary dimension must be fully known and experimentally characterized for every given QKD system, before it can be considered secure. Additionally, it is highly likely that environmental conditions change over time, invalidating these characterizations. For this reason, practical countermeasures at a protocol level are preferable to calibration-based approaches where possible.

B. Four-state countermeasure

In standard decoy-state BB84 QKD with time-bin/phase encoding, Alice uses an electro-optic modulator to encode a relative phase between a pair of optical pulses. Alice's phases,

$$\phi_A \in \left\{0,\frac{\pi}{2},\pi,\frac{3\pi}{2}\right\}, \tag{2}$$

encode the states typically denoted Z_0, X_0, Z_1, and X_1. Bob then demodulates with

$$\phi_B \in \left\{0,\frac{\pi}{2}\right\}, \tag{3}$$

corresponding to a measurement in the Z or X basis, respectively. The sum $\phi_A+\phi_B$ determines the interference Bob will achieve at his interferometer output: constructive or destructive if the phases sum to 0 or π respectively

(these contribute to sifted events), and random otherwise. This means that each *bit-and-basis* choice from Alice has a deterministic detector allocation, given that Bob's *basis* choice matched Alice's.

In the four-state countermeasure, the modulation values instead come from the same set of four phases for ϕ_B as ϕ_A [35]. The consequence of this is that now there are two possible combinations that will lead to a sifted bit for a given bit-and-basis choice at Alice. As long as the random choice of bit value at Bob is recorded, he can map his output sifted bits from the *physical* to *logical* register in postprocessing. On average, any detection-efficiency mismatch present between the physical detectors, regardless of the auxiliary degree of freedom responsible, should be erased in the logical detection events. As well as handling the static mismatch case described earlier, it should also shield the receiver against attacks from Eve that rely on exploiting the efficiency mismatch side-channel, for example with a faked-state attack [14].

The four-state countermeasure has been well studied from a theoretical perspective, and proven secure in [19]. However, to the best of our knowledge, the security of this technique has not yet been evaluated on experimental results. In the following, we replicate a time-shift attack on a gigahertz-clocked, fiber-based, phase-encoding QKD

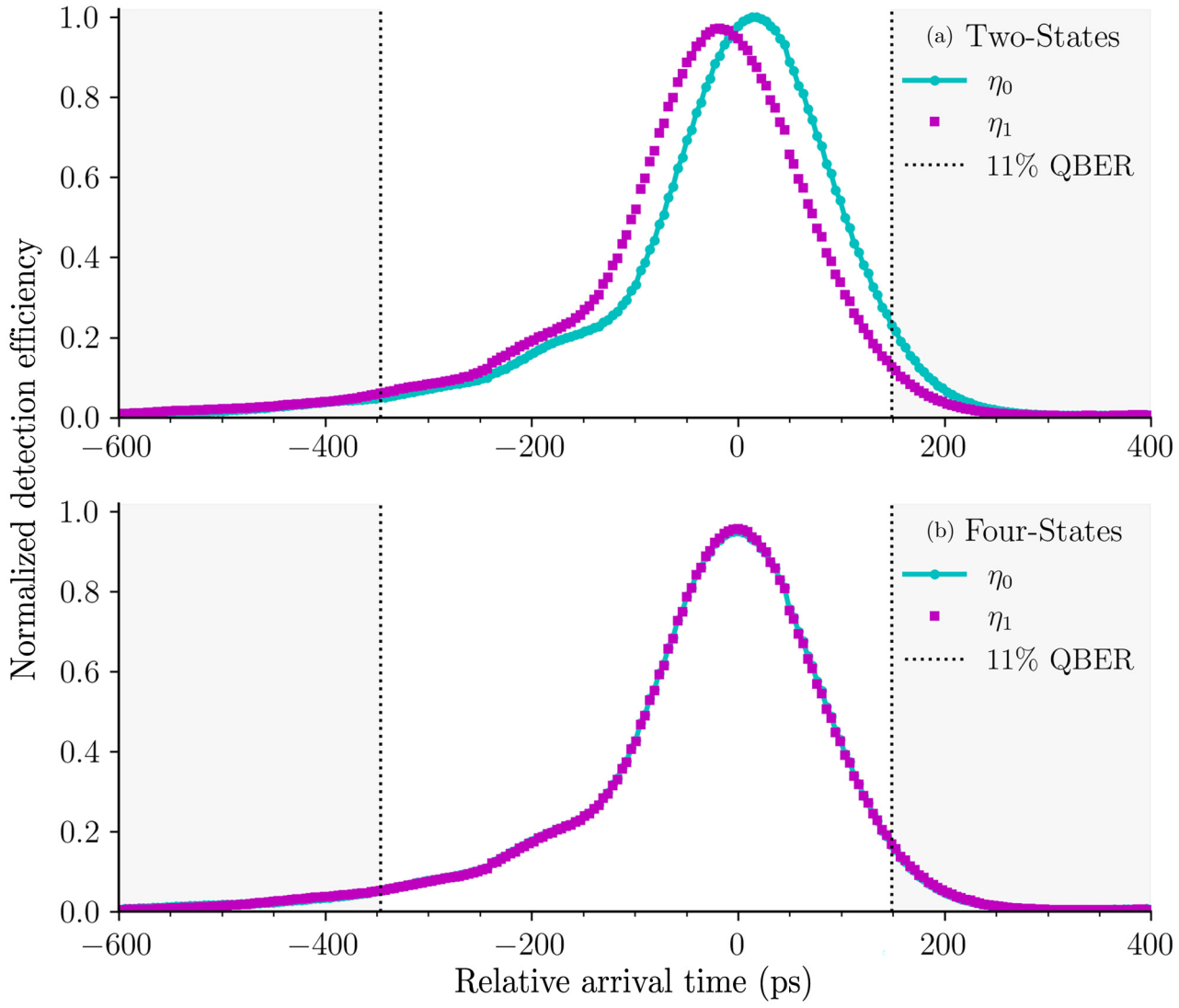

FIG. 2. Key components for experimental characterization of a fiber-based, gigahertz-clocked, phase-encoding QKD system's vulnerability to a time-shift attack. We sweep values of a relative delay, with resolution $\delta t = 4.5$ ps, and add this to the global reference clock's signal, which is then supplied to all active optical components in Bob, while recording counts from the APD outputs. LD, laser diode; ϕ_A, ϕ_B, phase modulators; Att., attenuation; λ, narrow-wavelength filter, here at 1550.12 ± 0.04 nm.

receiver, and compare the protocol's security in the cases that Bob demodulates with either two states or four states.

II. TIME-SHIFT ATTACK CHARACTERIZATION

In Fig. 2, we show key elements of the experimental setup we use to characterize the vulnerability of a fiber-based, gigahertz-clocked QKD system to a time-shift attack. The optical configuration in Alice is standard for phase-encoding BB84 QKD, composed of a gain-switched laser diode producing phase-randomized optical pulses, into which relative phases are encoded within an asymmetric Mach-Zehnder interferometer (AMZI), before being attenuated to single-photon intensity.

The receiver also contains standard optical components [36]. The phase modulator in Bob's AMZI can be programmed to use either two or four voltage levels. After the AMZI, each beam-splitter output is connected to a single-photon detector based on InGaAs APDs [30,32]. All active modulation components in both Alice and Bob, as well as Bob's APDs, are driven by local radio-frequency electronic driving signals. Alice and Bob are time-synchronized with each other by use of a global reference clock signal.

By delaying the electronic driving signals that control the phase modulator and APD gating windows in Bob, we can replicate the effects of the time-shift attack, as the pulse arrival time will be shifted with respect to the default modulation point. In our setup, we have separate control of the gating delays for Bob's phase modulator, APD 0, and APD 1, with a minimum resolution of 4.5 ps. We can therefore add or subtract delays with this resolution globally to all active components in the receiver.

As shown in Fig. 2, we took the outputs of each logical APD and recorded clicks across the two channels of a time-to-digital converter time tagger. In the case of the four-state countermeasure, the random bit-flip is undone in the post-processing hardware, which also handles enforced dead-times and basis sifting. At each time-shift, we recorded 10 Mb of total counts data.

This effect allows us to identify bounds on the time displacements applied, where the average QBER exceeds 11%, shown in Fig. 2. This is the most conservative cut-off where Alice and Bob can still distill a positive secret key [37] (note that the tolerable QBER is closer to 7% in real-world QKD with finite-size effects considered).

In Fig. 3 we show the bit-0 normalized detection bias with and without the countermeasure, defined as the contrast $((C_0 - C_1)/(C_0 + C_1))$, with C_0, C_1, the count rates for each APD. This data is a subset of that in Fig. 2, considering only the window inside the 11% QBER bounds. The four-state setting follows the ideal bias lined very closely across this window, but the bias varies significantly in the two-state case and reaches a maximum of approximately 30%. Again, error bars were too small to be visible.

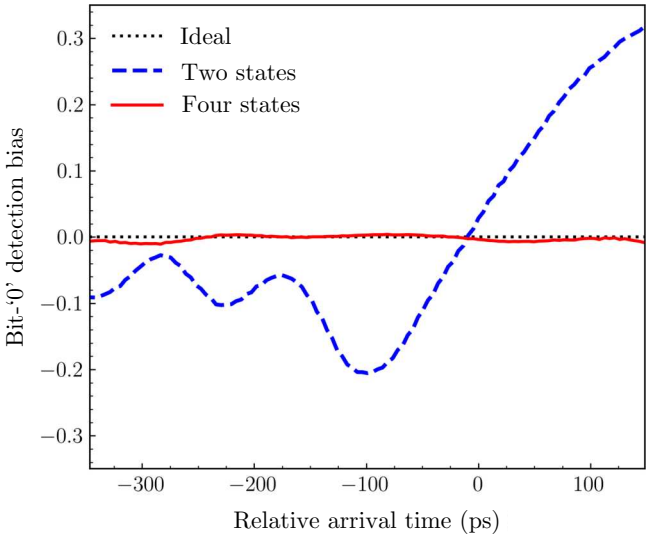

FIG. 3. Bit-0 normalized detection bias across a 495-ps window, in increments of 4.5 ps. While ideal APDs would exhibit no detection bias, the bias with two states varies significantly, to a maximum of approximately 30%. This data subset corresponds to the central region in Fig. 2, where average QBER was below 11%.

III. SECRET KEY RATE CALCULATIONS

The results from Fig. 2 and Fig. 3 suggest the four-state countermeasure comprehensively erases any effects of physical detection-efficiency mismatch in the sifted bits. To quantify the difference this would have on the secret key rates (SKRs) for our QKD protocol, we follow the original proof outlined by Fung *et al.* in [19] and built upon by Marcomini *et al.* [38], which utilizes the Procrustean method, a filtering technique from entanglement distillation theory that attempts to orthogonalize nonorthogonal single-photon input states [39].

The inputs to this method are two diagonal matrices for each APD's efficiency responses across the set of all arrival times, with the basis defined by the time-shift resolution δt; we obtain the diagonal elements directly from the results shown in Fig. 2. Following Marcomini *et al.*'s polarization-mismatch characterization results [38], where off-diagonal terms were roughly two orders of magnitude lower than the diagonal terms, we neglect off-diagonal contributions here.

The method then numerically bounds the probability of successful Procrustean filtering and the increased phase error rate associated with this filter, respectively p_{succ} and e_{phase}. We set up two constrained optimization problems using semidefinite programming (SDP) [40] to respectively minimize and maximize these values, subject to constraints that the phase and bit error rates due to Eve's actions must match those observed experimentally, $e_{\mathrm{phase,obs}}$ and $e_{\mathrm{bit,obs}}$. In the ideal case of no mismatch, we

TABLE I. Semidefinite program results and asymptotic secret key rates (R = secret bits per single photon received), showing the comparison between using time-shifts δt of 49.5 or 4.5 ps. Here we use $e_{\text{phase,obs}} = e_{\text{bit,obs}} = 0.03$ and $f_{\text{EC}} = 1.10$, for which $R_{\text{ideal}} = 0.592$.

	(a) $\delta t = 49.5$ ps	
	Two states	Four states
p_{succ}	0.609	0.981
e_{phase}	0.0475	0.0302
R	0.227	0.575
	(b) $\delta t = 4.5$ ps	
	Two states	Four states
p_{succ}	0.608	0.979
e_{phase}	0.0470	0.0303
R	0.228	0.574

have $p_{\text{succ}} = 1$ and $e_{\text{phase}} = e_{\text{phase,obs}}$. Otherwise, p_{succ} and e_{phase} are respectively decreased and increased, in proportion to the significance of the efficiency mismatches across all time-shifts considered, again taken from the data subset shown displayed in Fig. 3.

The asymptotic SKR is computed, using values returned from the SDP, with

$$R = \left[p_{\text{succ}}(1 - H_2(e_{\text{phase}})) - f_{\text{EC}} H_2(e_{\text{bit}})\right], \qquad (4)$$

where $H_2(x)$ is the binary entropy function, and f_{EC} is the efficiency of classical error correction. In the ideal case, using QBERs of $e_{\text{phase,obs}} = e_{\text{bit,obs}} = 0.03$ and $f_{\text{EC}} = 1.10$ [36], the maximum achievable rate is $R = 0.592$. The corresponding rates for the four-state and two-state cases are shown in Table I(b). The four-state results recovers 97.1% of the ideal SKR, while the rate is cut to 38.3% of the ideal SKR in the two-state case.

In Fig. 4, we compare how the asymptotic SKR performs with loss for these three scenarios. Here, the rate on detected single photons from Eq. (4) is scaled by a prefactor η, encompassing channel transmissivity and total detection efficiency, with the observed error rates simulated as a function of loss, due to the contributions of dark counts. Again, we see the four-state case very closely recovers the ideal SKR.

A. Minimum resolution of characterization

The proof by Fung *et al.* [19] requires a narrow-wavelength filter to be present at both the output of Alice and the input of Bob, when characterizing the QKD system's vulnerability to the time-shift attack. This allows the Hilbert space to be treated as finite-dimensional, where in reality time is a continuous variable and a time-shift attack is possible with arbitrary resolution.

We tested the accuracy of this assumption by using a higher-resolution sampling rate. The filter bandwidth in

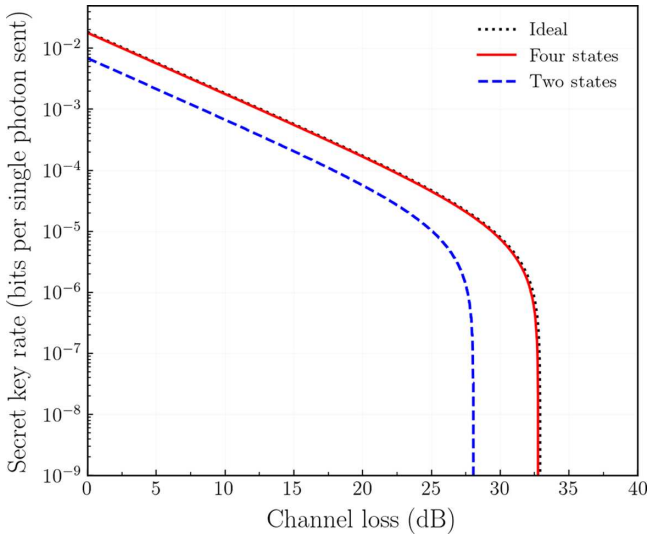

FIG. 4. Asymptotic secret key rates (SKRs) in bits per single photon sent against channel loss, accounting for detection-efficiency mismatch. The four-state countermeasure recovers 97.1% of the ideal case of no mismatch, while the rate is reduced to 38.3% of ideal in the two-state case.

our setup was 10 GHz at 1550.12 nm, from which a minimum sampling resolution of 50 ps is derived, using the Nyquist-Shannon sampling theorem. The experiment was performed using time-shifts of $\delta t = 4.5$ ps, from which a set of subsampled shifts with $\delta t = 49.5$ ps could be extracted. In Table I, we compare the two resolutions, showing the results of the SDP and the SKR computed using Eq. (4) in each case. Approximately equivalent values were obtained, validating the finite-dimensional filter-based characterization approach.

IV. DISCUSSION

We have demonstrated the practical security of the four-state countermeasure in a phase-encoding prototype QKD system. We have shown that the ideal SKR is almost completely recovered using this countermeasure despite the presence of severe physical detection-efficiency mismatch, while the standard BB84 detector operation would see an extreme performance reduction. Our results provide strong justification for the adoption of this countermeasure as standard for future scalable and practical commercial, BB84-style, QKD systems.

Furthermore, our experimental verification of this technique's high performance is a substantial achievement, due to the high-speed nature of our implementation. At gigahertz clock rates, it is not trivial to achieve the required phase modulation cleanly and with low residual error rates. This distinguishes our demonstration from earlier work that reported usage of four-state demodulation with clock rates in the megahertz range [23]. We note that the technique may introduce a very slight increase in QBER, even

under default QKD operation with the APD gating at their optimum timing alignments, likely due to the fact agreement is now required between Alice and Bob's phase modulator levels for two pairs of voltage levels rather than one.

As mentioned previously, security proofs now exist that account for detection-efficiency mismatches with more realistic assumptions, including the incorporation of the decoy-state technique [21,31,33,41], and finite-size effects [34]. Future work could extend the analysis on results obtained from our experimental data, using more recent proof techniques.

However, while such proofs can explicitly quantify potential information leakage, we reiterate that for an implementation issue as broad and multifaceted as detection-efficiency mismatch, it is highly impractical to perform sophisticated characterizations, such as the one presented in this paper, for all possible auxiliary degrees of freedom (temporal, wavelength-based, and polarization-based mismatches, etc. [42]), for every single QKD system produced. Yet, this is what existing approaches require to guarantee secure operation, because each system will have a unique pair of single-photon detectors.

On the other hand, the design-level robustness of the four-state countermeasure allows the same technique to be applied uniformly to all QKD systems, requiring one additional random number per clock cycle at the receiver in compensation for this significant practical advantage. A further crucial difference to stress is that the principle of symmetrizing logical detection events across the physical detection devices means that a QKD system can continue to securely generate a key in the presence of severe mismatched detection efficiencies, even down to the case of using only a single detector in the receiver. The mismatch probed in our experiment was chosen to emulate the original time-shift attack results [18], but previous work shows eavesdropping strategies that exploit device calibration routines can induce extreme temporal mismatches [43], an attack vector against which only a QKD system using the four-state countermeasure would be resilient. A characterization-based proof approach, on the contrary, would not allow for any positive key to be established beyond a certain degree of mismatch.

A common criticism of this countermeasure is that it is vulnerable to a Trojan horse attack on the receiver [19,20], where Eve could read out Bob's phase modulator choices from the reflections of a bright light injection attack. Yet, techniques to protect against a Trojan horse attack are well known, for example using fiber delays [44], optical isolation, wavelength filters, and watchdog detectors [45], and are required in a QKD system regardless of the modulation settings Bob uses. Hence, we are unaware of any *new* side-channel that is opened up with the four-state countermeasure. We further stress that a practical time-shift attack is feasible with existing technology [42], and should correspondingly be considered the highest threat. Closing the most accessible loopholes available to a quantum hacker, and thereby forcing them to resort to a more difficult and limited set of attacks, is significant progress in implementation security.

Finally, we caveat that the four-state countermeasure will not to be applicable to all QKD receivers and protocols. Previous analysis of free-space polarization-encoding QKD has shown that detection-efficiency mismatch can still be present when all spatial modes are considered [46], a side-channel that does not exist in single-mode fiber.

ACKNOWLEDGMENTS

B.T. gratefully acknowledges funding from the Engineering and Physical Sciences Research Council. Toshiba Europe Limited. would like to acknowledge funding from Innovate UK's QAssure project (10102791). M.L. would like to acknowledge the Engineering and Physical Sciences Research Council Integrated Quantum Networks Hub (EP/Z533208/1). The authors thank Evan Lavelle for hardware support. B.T. thanks Joseph Dolphin, Martin Ward, and Matthew Winnel for helpful discussions.

DATA AVAILABILITY

The data that support the findings of this article are not publicly available because they contain commercially sensitive information. The data are available from the authors upon reasonable request.

[1] J. F. Dynes, A. Wonfor, W. W.-S. Tam, A. W. Sharpe, R. Takahashi, M. Lucamarini, A. Plews, Z. L. Yuan, A. R. Dixon, J. Cho, Y. Tanizawa, J.-P. Elbers, H. Greißer, I. H. White, R. V. Penty, and A. J. Shields, Cambridge quantum network, npj Quantum Inf. **5**, 101 (2019).

[2] M. Sasaki *et al.*, Field test of quantum key distribution in the Tokyo QKD Network, Opt. Express **19**, 10387 (2011).

[3] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, Rev. Mod. Phys. **92**, 025002 (2020).

[4] N. Lütkenhaus and M. Jahma, Quantum key distribution with realistic states: Photon-number statistics in the photon-number splitting attack, New J. Phys. **4**, 44 (2002).

[5] J. F. Dynes, M. Lucamarini, K. A. Patel, A. W. Sharpe, M. B. Ward, Z. L. Yuan, and A. J. Shields, Testing the photon-number statistics of a quantum key distribution light source, Opt. Express **26**, 22733 (2018).

[6] H.-K. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **108**, 130503 (2012).

[7] L. C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, A. W. Sharpe, S. W.-B. Tam, Z. L. Yuan, R. V. Penty, and A. J. Shields, Quantum key distribution without detector vulnerabilities using optically seeded lasers, Nat. Photonics **10**, 312 (2016).

[8] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate–distance limit of quantum key distribution without quantum repeaters, Nature **557**, 400 (2018).

[9] V. Zapatero, T. van Leent, R. Arnon-Friedman, W.-Z. Liu, Q. Zhang, H. Weinfurter, and M. Curty, Advances in device-independent quantum key distribution, npj Quantum Inf. **9**, 10 (2023).

[10] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, Theor. Comput. Sci. **560**, 7 (2014). Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

[11] 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).

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

[13] B. Gao, Z. Wu, W. Shi, Y. Liu, D. Wang, C. Yu, A. Huang, and J. Wu, Ability of strong-pulse illumination to hack self-differencing avalanche photodiode detectors in a high-speed quantum-key-distribution system, Phys. Rev. A **106**, 033713 (2022).

[14] V. Makarov and J. Skaar, Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols, Quantum Inf. Comput. **8**, 622 (2008). Rinton Press, Incorporated.

[15] 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).

[16] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Trojan-Horse attacks on quantum-key-distribution systems, Phys. Rev. A **73**, 022320 (2006).

[17] I. S. Sushchev, D. S. Bulavkin, K. E. Bugai, A. S. Sidelnikova, and D. A. Dvoretskiy, Trojan-Horse attack on a real-world quantum key distribution system: Theoretical and experimental security analysis, Phys. Rev. Appl. **22**, 034032 (2024).

[18] 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).

[19] 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).

[20] V. Makarov, A. Anisimov, and J. Skaar, Effects of detector efficiency mismatch on security of quantum cryptosystems, Phys. Rev. A **74**, 022313 (2006).

[21] L. Lydersen and J. Skaar, Security of quantum key distribution with bit and basis dependent detector flaws, Quantum Inf. Comput. **10**, 60 (2010).

[22] P. M. Nielsen, C. Schori, J. L. Sorensen, L. Salvail, I. Damgard, and E. Polzik, Experimental quantum key distribution with proven security against realistic attacks, J. Mod. Opt. **48**, 1921 (2001).

[23] S. Wang, W. Chen, Z.-Q. Yin, Y. Zhang, T. Zhang, H.-W. Li, F.-X. Xu, Z. Zhou, Y. Yang, D.-J. Huang, L.-J. Zhang, F.-Y. Li, D. Liu, Y.-G. Wang, G.-C. Guo, and Z.-F. Han, Field test of wavelength-saving quantum key distribution network, Opt. Lett. **35**, 2454 (2010).

[24] M. Lucamarini, Implementation security of quantum cryptography - introduction, challenges, solutions, ETSI White Paper No. 27 (2018).

[25] T. Ferreira da Silva, G. C. do Amaral, G. B. Xavier, G. P. Temporão, and J. P. von der Weid, Safeguarding Quantum Key Distribution Through Detection Randomization, IEEE J. Sel. Top. Quantum Electron. **21**, 159 (2015).

[26] M. A. Ruhul Fatin and S. Sajeed, Generalized efficiency mismatch attack to bypass the detection-scrambling countermeasure, Opt. Express **29**, 16073 (2021).

[27] V. Makarov, A. Abrikosov, P. Chaiwongkhot, A. K. Fedorov, A. Huang, E. Kiktenko, M. Petrov, A. Ponosova, D. Ruzhitskaya, A. Tayduganov, D. Trefilov, and K. Zaitsev, Preparing a commercial quantum key distribution system for certification against implementation loopholes, Phys. Rev. Appl. **22**, 044076 (2024).

[28] D. Rusca and N. Gisin, Quantum Cryptography: An Overview of Quantum Key Distribution, arXiv:2411.04044.

[29] N. Jain, B. Stiller, I. Khan, D. Elser, C. Marquardt, and G. Leuchs, Attacks on practical quantum key distribution systems (and how to prevent them), Contemp. Phys. **57**, 366 (2016).

[30] R. H. Hadfield, Single-photon detectors for optical quantum information applications, Nat. Photonics **3**, 696 (2009).

[31] A. Trushechkin, Security of quantum key distribution with detection-efficiency mismatch in the multiphoton case, Quantum **6**, 771 (2022).

[32] J. Zhang, M. A. Itzler, H. Zbinden, and J.-W. Pan, Advances in InGaAs/InP single-photon detector systems for quantum communication, Light: Sci. Appl. **4**, e286 (2015).

[33] F. Grasselli, G. Chesi, N. Walk, H. Kampermann, A. Widomski, M. Ogrodnik, M. Karpiński, C. Macchiavello, D. Bruß, and N. Wyderka, Quantum key distribution with basis-dependent detection probability, Phys. Rev. Appl. **23**, 044011 (2025).

[34] D. Tupkary, S. Nahar, P. Sinha, and N. Lütkenhaus, Phase error rate estimation in QKD with imperfect detectors, Quantum **9**, 1937 (2025).

[35] M. LaGasse, Secure use of a single single-photon detector in a QKD system, https://patents.google.com/patent/US20050190922A1/en (2005).

[36] Z. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A. W. Sharpe, A. R. Dixon, E. Lavelle, J. F. Dynes, A. Murakami, M. Kujiraoka, M. Lucamarini, Y. Tanizawa, H. Sato, and A. J. Shields, 10-Mb/s Quantum Key Distribution, J. Lightwave Technol. **36**, 3427 (2018). Conference Name: Journal of Lightwave Technology.

[37] P. W. Shor and J. Preskill, Simple Proof of Security of the BB84 Quantum Key Distribution Protocol, Phys. Rev. Lett. **85**, 441 (2000).

[38] A. Marcomini, A. Mizutani, F. Grünenfelder, M. Curty, and K. Tamaki, Loss-tolerant quantum key distribution with detection efficiency mismatch, Quantum Sci. Technol. **10**, 035002 (2025).

[39] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Concentrating partial entanglement by local operations, Phys. Rev. A **53**, 2046 (1996).

[40] P. Skrzypczyk and D. Cavalcanti, *Semidefinite Programming in Quantum Information Science* (IOP Publishing, 2023).

[41] 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. Res. **3**, 013076 (2021).

[42] *BSI Implementation Attacks against QKD Systems*, Tech. Rep. (2023). https://www.bsi.bund.de/EN/Service-Navi/Publikationen/Studien/QKD-Systems/Implementation_Attacks_QKD_Systems_node.html.

[43] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, Device Calibration Impacts Security of Quantum Key Distribution, Phys. Rev. Lett. **107**, 110501 (2011).

[44] A. R. Dixon, J. F. Dynes, M. Lucamarini, B. Fröhlich, A. W. Sharpe, A. Plews, W. Tam, Z. L. Yuan, Y. Tanizawa, H. Sato, S. Kawamura, M. Fujiwara, M. Sasaki, and A. J. Shields, Quantum key distribution with hacking countermeasures and long term field trial, Sci. Rep. **7**, 1978 (2017).

[45] M. Lucamarini, I. Choi, M. Ward, J. Dynes, Z. Yuan, and A. Shields, Practical Security Bounds Against the Trojan-Horse Attack in Quantum Key Distribution, Phys. Rev. X **5**, 031030 (2015).

[46] M. Rau, T. Vogl, G. Corrielli, G. Vest, L. Fuchs, S. Nauerth, and H. Weinfurter, Spatial Mode Side Channels in Free-Space QKD Implementations, IEEE J. Sel. Top. Quantum Electron. **21**, 187 (2015).