suggests that setting appropriate detector discrimination levels would be sufficient to prevent the detector blinding attack on the QPN5505 and Clavis2 QKD systems.

It is worth pointing out that gain modulation of the photocurrent will also be sufficient to prevent the thermal attack[7] on APDs. This attack uses high CW powers to generate a photocurrent that heats the APD and thereby increases V_b. Considering the required optical power (>1 mW)[7], a slight modulation in gain is sufficient for persistent counting. Indeed we have confirmed the absence of any thermal blinding effect with an optical excitation of 17.8 mW, which corresponds to a heating power of 500 mW in the APD.

Finally, it is important to emphasize that any attack with strong illumination will result in a large photocurrent. Monitoring the photocurrent for anomalously high values is a straightforward way of detecting any attack of this type. This is applicable to all types of APDs, including those that are ungated[5] or used in high-speed gated mode[3,4], and can therefore be used to reveal bright illumination attacks on QKD systems using APDs. ❐

References
1. Lydersen, L. *et al. Nature Photon.* **4,** 686–689 (2010).
2. Bethune, D. S. & Risk, W. P. *IEEE J. Quant. Electron.* **36,** 340–347 (2000).
3. Namekata, N., Sasamori, S. & Inoue. S. *Opt. Express* **14,** 10043–10049 (2006).
4. Yuan, Z. L., Kardynal, B. E., Sharpe, A. W. & Shields, A. J. *Appl. Phys. Lett.* **91,** 041114 (2007).
5. Makarov, V. *New J. Phys.* **11,** 065003 (2009).
6. Gobby, C., Yuan, Z. L. & Shields, A. J. *Appl. Phys. Lett.* **84,** 3762–3764 (2004).
7. Lydersen, L. *et al.* Preprint at http://arxiv.org/abs/1009.2663v1 (2010).

Additional information

The authors declare competing financial interests: details accompany the paper at www.nature.com/naturephotonics.

Z. L. Yuan, J. F. Dynes and A. J. Shields*
Toshiba Research Europe, Cambridge Research Laboratory, 208 Cambridge Science Park, Milton Road, Cambridge CB4 0GZ, UK.
*e-mail: andrew.shields@crl.toshiba.co.uk; zhiliang.yuan@crl.toshiba.co.uk

Lydersen *et al.* reply: We are glad that our results have improved awareness and stimulated discussions concerning the imperfections of detectors, particularly among the leading research groups that use APDs in QKD systems. Yuan *et al.* propose a method to avoid the blinding of gated APD-based detectors, such as those used in the two commercial QKD systems addressed in our recent publication[1]. Our experimental data from Clavis2 indicate that the countermeasure suggested by Yuan *et al.* will make it more difficult to blind gated detectors.

However, for gated detectors, avoiding blinding is insufficient to avoid our attack. Gated detectors operate in linear mode between the gates, and the trigger pulse can therefore be applied directly after the gate (discarding these clicks based on arrival times seems to be impractical because of detector jitter). We remarked that this causes afterpulses[1], but in fact the after-gate attack can fully compromise the security for a wide range of system parameters[2]. Even outside this range, one must quantify in a proof-of-security how well Eve may perform. Removing the bias resistor and lowering the comparator threshold does not avoid exploiting the linear mode between gates. In fact, lowering the comparator threshold reduces the required trigger pulse power, and thus probably improves the after-gate attack by reducing afterpulsing.

Furthermore, it seems that the detectors can still be blinded even with the changes proposed by Yuan *et al.*; simply removing the bias resistor has turned out to be insufficient. In our recent paper[3], we removed the bias resistor from Clavis2 but were still able to blind the detectors in several ways. Yuan *et al.* did not observe thermal blinding from continuous-wave illumination. This may be due to the lower comparator threshold and/or insufficient heating, as they illuminate only one APD instead of two, while operating at a higher temperature, which effectively increases the cooler capacity.

Even if the bias resistor is removed and the discrimination level is set just above the capacitive charging signal, the detectors seem to be vulnerable to sinkhole blinding[3]. In sinkhole blinding, the APD is illuminated between the gates. With a suitable duty cycle of the blinding illumination, it should be straightforward to blind the detector while keeping the comparator input well below the amplitude of the capacitive signal.

Monitoring the photocurrent of the APDs is like using a power meter at Bob's entrance, which we discussed in our original paper[1]. Furthermore, this will not reveal the after-gate attack.

It seems that the countermeasure proposed by Yuan *et al.* does not prevent our general attack of tailored bright illumination. So far, we have been able to blind and control every APD-based detector that we have looked at thoroughly (albeit with different techniques), including three different passively quenched detectors[4], one actively quenched detector[5] and two different gated detectors[1–3].

In our opinion, this discussion shows how important it is to close the QKD security loophole in a thorough and provable way. We doubt that this can be achieved efficiently in small increments of intuitive patches, which will cause rapid iterations and so force manufacturers to update their QKD systems frequently. We are confident that APD-based single-photon detectors can be, and will be, made secure by a proper implementation of QKD combined with a sufficiently general security proof.

As a final remark, we want to emphasize that in our experiments[1–3] the QKD systems were treated as black boxes, just as they would be for Eve. We reverse-engineered the detector circuitries (realistically, Eve can buy a copy of Bob and do the same) and non-intrusively recorded the detector response during our experiments. Clavis2 shipped with its factory settings ready for QKD, including the discrimination level, which we used for our experiments. As pointed out in our Supplementary Information[1], QPN 5505 did not ship with factory settings, but we followed the manual and used the settings that gave us the best QKD performance. ❐

References
1. Lydersen, L. *et al. Nature Photon.* **4,** 686–689 (2010).
2. Wiechers, C. *et al.* Preprint at http://arxiv.org/abs/1009.2683v1 (2010).
3. Lydersen, L. *et al.* Preprint at http://arxiv.org/abs/1009.2663v1 (2010).
4. Makarov, V. *New J. Phys.* **11,** 065003 (2009).
5. Makarov, V., Anisimov, A. & Sauge, S. Preprint at http://arxiv.org/abs/0809.3408v2 (2010).

Lars Lydersen[1,2], Carlos Wiechers[3,4,5], Christoffer Wittmann[3,4], Dominique Elser[3,4], Johannes Skaar[1,2] and Vadim Makarov[1]
[1]Department of Electronics and Telecommunications, Norwegian University of Science and Technology, NO-7491 Trondheim, Norway. [2]University Graduate Center, NO-2027 Kjeller, Norway. [3]Max Planck Institute for the Science of Light, Günther-Scharowsky-Strasse 1/Bau 24, 91058 Erlangen, Germany. [4]Institut für Optik, Information und Photonik, University of Erlangen-Nuremberg, Staudtstrasse 7/B2, 91058 Erlangen, Germany. [5]Departamento de Física, Universidad de Guanajuato, Lomas del Bosque 103, Fraccionamiento Lomas del Campestre, 37150, León, Guanajuato, Mexico.
e-mail: lars.lydersen@iet.ntnu.no