

Modified photodiodes advance quantum communications

Princeton Lightwave has launched a single-photon avalanche photodiode that is targeting quantum cryptography applications. **Mark Itzler** describes some of the benefits it offers that result from the device's design, and the advantages it has over rival detectors.

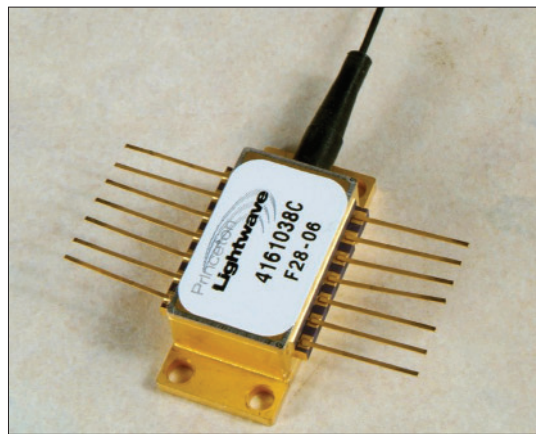
Until recently one of the primary challenges faced by cryptographers was the secure exchange of encryption keys. Although secure messages could be easily transmitted between two parties once they possessed the same key for encrypting and decrypting messages, it was difficult to devise an efficient and secure method of transferring the key between them.

The advent of public network encryption has revolutionized secure information exchange. This modern method, based on algorithms, involves one party providing a public key that allows any other party to encrypt a message, but decryption can only be performed with a separate, private key held by the first party. This scheme does have a weakness, though, because it relies on computational complexity. Although breaking the key is exceedingly difficult today, this data encryption approach could be compromised in the foreseeable future through advances in computational power and the mathematics associated with code breaking.

However, the future for secure communication is not under threat because a truly unbreakable digital data encryption method also exists, which has been developed over the last 20 years and exploits the quantum mechanical properties of photons (see "Quantum key distribution systems" box, pXX). Recently, commercial point-to-point secure links using quantum key distribution (QKD)-based encryption techniques have been launched from a handful of start-up companies, including idQuantique in Switzerland and MagiQ Technologies in the US. In addition, several large Japanese corporations, including Mitsubishi, NEC and Toshiba, have product-oriented programs for QKD system development.

These QKD systems are similar to traditional optical communications systems, and contain optical sources and detectors. However, QKD systems require single-photon transmission and detection, and the transmission of single photons currently limits QKD implementation to single-span point-to-point links, because single-photon repeaters that faithfully maintain the photon's quantum mechanical properties are not available.

Another obstacle that restricts the performance of current QKD links is the lack of available high-quality



Princeton Lightwave's single-photon avalanche diode (SPAD)-based receivers have to combine a high level of performance with accommodation for the optical, thermal and electrical interfaces. To provide high coupling efficiency with single-mode fiber, the design uses sub-micron fiber alignment to small active-area devices that are thermoelectrically cooled and housed in a standard 14 pin butterfly-type package.

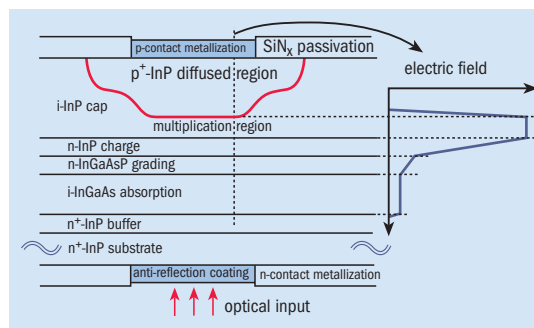
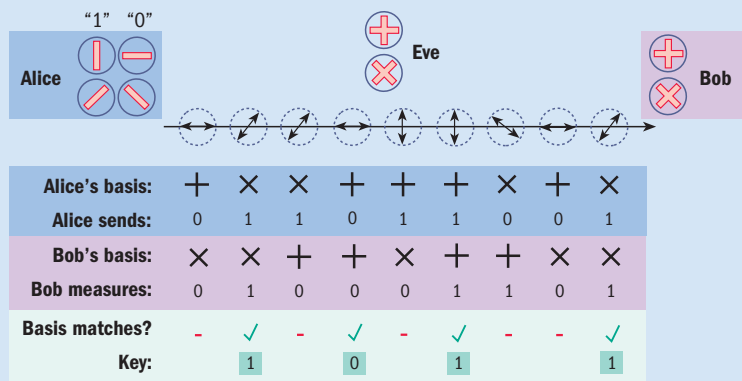


Fig. 1. Princeton Lightwave's SPADs, like linear-mode avalanche photodiodes, use a doped charge layer to maintain a high field, which generates the avalanche gain in the multiplication region while keeping sufficiently low field in the absorption region to minimize field-induced leakage currents.

single-photon detectors. To meet this need, at Princeton Lightwave we have recently developed the first commercially available InGaAs/InP-based single-photon avalanche diode (SPAD), which is also used in our single-photon benchtop receiver, incorporating the necessary electronic control circuitry.

Our detector outperforms photomultiplier tubes for QKD applications because these devices have a single-photon detection efficiency of only around 1%. It is also more suitable for QKD than the commercial linear-mode avalanche photodiodes (APDs) that detect between 0.3 and 1.6 μm and are used as SPADs by many of today's photon-counting practitioners. These APDs can deliver single-photon counting performance when biased above the breakdown voltage, V_{br} , because a single photoexcited carrier can induce a runaway avalanche that leads to an easily detectable

Quantum key distribution systems



In quantum key distribution systems each data bit is represented by a single photon assigned a value using a quantum mechanical variable such as polarization. In the example above, this allows Alice and Bob to communicate by choosing a particular value for the polarization of each bit, using values taken from one of two randomly chosen quantum mechanical “bases”, represented by horizontal/vertical polarizations and +45°/−45° polarizations. In each basis, one polarization direction corresponds to a digital “1” and the other to a “0”.

Alice, the sender, prepares a photon with the correct polarization for her first bit value (1 or 0). If Bob’s randomly chosen basis matches Alice’s, he measures the correct bit value. However, if he chooses the wrong basis, quantum mechanics dictates that there is a 50% chance he will measure the intended bit value and a 50% chance he measures the wrong value. After receiving all the information, Bob informs Alice via an insecure channel which basis he has used to measure each photon. Alice responds by telling Bob for which bits his basis choice was correct, and these bits are used as the encryption key.

This method is absolutely secure because it is impossible for an eavesdropper, known as the nefarious Eve to cryptographers everywhere, to intercept the key. To try and break the code she has to randomly choose a polarization basis for each photon measurement, just as Bob does, but even if she monitors Alice and Bob’s public discussion concerning their choices of basis, her random basis choices differ from Bob’s.

Eve’s situation is further disadvantaged because she can not intercept photons during the key distribution process without being detected. Even if she attempts to replace intercepted single photons, her incorrect polarization bases will mean that her replacement photons are not equivalent to Alice’s. Eve’s meddling is exposed when Alice and Bob check the validity of their transmitted key through error checking procedures, and the corrupted key is discarded.

macroscopic current. However, although these devices occasionally offer a good SPAD performance, they usually behave rather poorly because they are not designed for this application. They also have tremendous performance variations when used as SPADs, such as dark count rates (DCRs) that differ by several orders of magnitude.

APD design similarities...

Our SPADs share many device design elements with linear-mode APDs (see figure 1). For example, they incorporate an In_{0.53}Ga_{0.47}As layer that provides an acceptable absorption up to 1.65 μm at room temperature and a wider bandgap InP multiplication region, because it is not possible to deliver high-field avalanche gain in InGaAs without also generating large leakage currents. Inserted between these is an InP field control layer, which enables the device to maintain high and low fields in the multiplication and absorp-

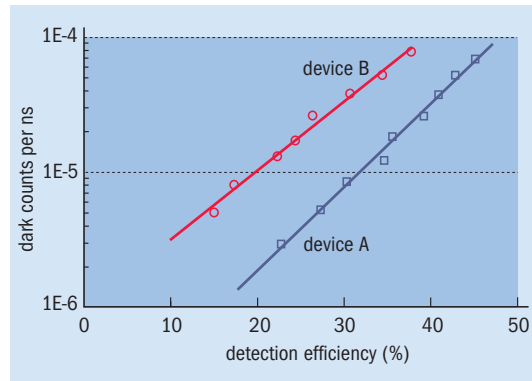


Fig. 2. Two of Princeton Lightwave’s devices that have a 25 μm diameter active area show the expected trade-off between dark count rate (DCR) and detection efficiency. Device A has a lower DCR at a given single-photon detection efficiency than device B, but at the expense of higher timing jitter. For device A, a lower electric field in the absorption region leads to a lower DCR value due to reduced tunneling, but this also adversely impacts the carrier dynamics, which leads to a higher timing jitter. Both devices were operated at 200 K with active quenching and a 10 kHz gate repetition rate.

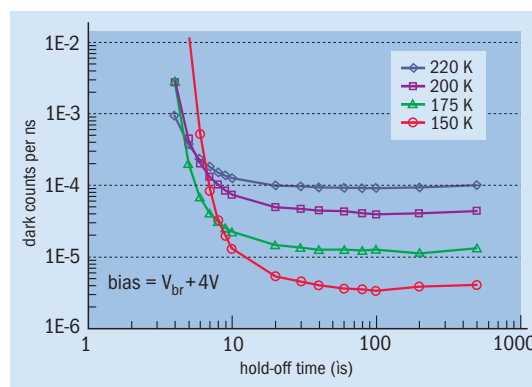


Fig. 3. The dark count rates of Princeton Lightwave’s 40 μm diameter SPADs illustrate the adverse effects of short hold-off times that lead to afterpulsing effects. These devices were operated with 20 ns gate time, gated quenching and an operating bias 4 V above the breakdown voltage.

tion regions, respectively. Since a direct InGaAs/InP interface can trap carriers, a grading is added to smooth this interface.

...and differences

Despite the structural similarities, SPADs and linear-mode APDs do differ significantly. APDs require thin multiplication regions to reduce linear-mode APD noise and produce a more deterministic linear-mode avalanche process, while SPADs benefit from thicker multiplication regions that increase the probability of generating self-sustaining avalanches. SPAD designs must also be compatible with −60 °C or lower operating temperatures, which reduce the dark count rate. Lastly, the design has to reflect the device’s detection process – linear-mode APDs are used as analog devices, but SPADs trigger a digital threshold circuit.

For linear-mode APDs the quantum efficiency is determined by the proportion of the photons that are

absorbed and then create photoexcited carriers. For SPADs, though, the carriers must also induce a detectable runaway avalanche, and it is the product of the probabilities of these two processes that determines the single-photon detection efficiency (SPDE).

The SPAD performance can be degraded by “dark counts” caused by processes other than photoexcitation, such as thermal excitation and the field-mediated creation of free carriers. To minimize these effects the devices are usually operated in gated mode. The detector is biased just below V_{br} , and a gate pulse is then applied to bring the detector bias above breakdown for a typically 1–100 ns. After the avalanche is initiated and detected, it is quenched to allow the SPAD to be reset to its armed state with another gate pulse.

Effective QKD systems also demand minimal variation in the time taken for the detection of a photon. The main contribution to the timing jitter for single-photon detection is a fluctuation in the way a runaway avalanche spreads laterally across the active area of a SPAD, but this variation can be reduced by using a higher bias voltage. SPADs also suffer from an after-pulsing effect that occurs when carriers created during an avalanche are trapped by defects in the multiplication region, and freed later through processes such as thermal emission, which contribute to the dark count. However, this unwanted effect can be compensated for by increasing the “hold-off” time before the next gate.

Working devices

The SPADs we have fabricated at Princeton Lightwave show that there is a trade-off between two important parameters, the SPDE and the DCR (see figure 2). While the SPDE improves linearly with increasing bias above V_{br} , the DCR also increases exponentially with increasing bias. The DCR can be reduced by cooling the device, but the required hold-off time increases (see figure 3).

At the system level this means that faster repetition rates are only possible at higher DCR. However, this is not a current concern for QKD systems as many of today’s secure point-to-point links use manual key distribution with timeframes of weeks or even months between key updates, while commercial QKD systems already provide new encryption keys with absolute security in just a fraction of a second.

We expect QKD deployment to continue to grow as the relevant component technologies mature, with SPADs playing a key role in improving system performance. We will focus on device performance improvements that raise the SPDE and lower the DCR because we believe that the QKD link reach is currently limited by SPAD’s DCR performance and that the single-photon transmission rate is restricted by the SPDE. ●

● *We wish to thank Radu Ispasoiu and Sergio Cova for device characterization and insightful discussions.*



About the author

Mark Itzler is chief technical officer at Princeton Lightwave. He previously held the equivalent role at the EPITAXX division of JDS Uniphase.