Toshiba makes cryptography video breakthrough

Medical Design Technology

Scientists at Toshiba Research Europe's Cambridge Laboratory in the UK have provided new quantum key distribution (QKD) equipment to demonstrate the first ultra-secure video conference call based on the photonic technology.

Quantum cryptography is a secure method of distributing digital encryption keys across an optical fiber network. Thanks to the rules of quantum mechanics, anyone intercepting the key is detected and the security of the communication link is not compromised.

But with users placing an ever greater demand on bandwidth, the problem facing the Toshiba team has been to increase the rate at which those keys can be exchanged. For example, secure video links require rates on the order of hundreds of kilobits per second, a big step up from voice communication, which requires rates of only a few kb/sec.

Secure video conference
In a field trial in Japan in October organised by the National Institute of Information and Communications Technology, Toshiba successfully demonstrated the highest bit rate to date for QKD on installed fiber. *"We demonstrated a system delivering 300 kb/sec of key material over a 45 km link,"* **Andrew Shields**, the Assistant Managing Director of Toshiba Research Europe, told optics.org. *"This meant that we could perform one-time pad encryption of video for the first time and were able to have a secure video conference."*

One-time pad is an encryption algorithm and the only known method that is theoretically perfectly secret. Although ultra-secure, the application of one-time pad encryption has been restricted in the past as it requires one bit of key for every one bit of data. In other words, each key has to be the same length as the data. For this reason it has only been used for short messages in situations requiring very high security, for example by the military and security services. Demonstrations such as the secure video link however pave the way for QKD to be used in everyday situations.

A major advance in detector technology was behind the improved bit rate and the success of the video link trial. While a conventional avalanche photodetector (APD) counts photons at a rate of only a few MHz, Shields and his team at Toshiba have now developed a self-differencing avalanche photodiode (SD-APD) that operates at 500Mcounts per second.

Toshiba's SD-APD overcomes the key issue of "dead time". Conventional APDs have to be operated with a long dead time because avalanche carriers can become trapped by defects in the semiconductor detector material. A long dead time ensures that these carriers decay back into a lower energy band without producing

a second spurious click.

"We have found a way to detect much weaker avalanches by cancelling out nearly all of the background noise," explained **Shields**. *"Weaker avalanches mean that there is less trapping of carriers and we no longer need the long dead time. Previously, we required a dead time of 250 ns between each detection event, limiting the detection rate to 4 MHz. Now we can detect a photon every 2 ns, so 500 MHz [is possible]."*

Overcoming detector blinding

In a related development, the Toshiba team has also been able to address a potential weakness of QKD that had been proposed by Lars Lydersen and his colleagues from the Norwegian University of Science and Technology in Trondheim. In a paper entitled "Hacking commercial quantum cryptography systems by tailored bright illumination" (Nature Photonics 4 686), they suggested a way to blind APDs. The idea involved shining bright light onto the APD so that it could not detect single photons. It would then be possible to force so-called "detection events", in essence hacking the QKD system.

Intrigued by this paper, the Shields group decided to recreate the attack but found that it was only successful if a redundant resistor was included in series with the single-photon detector, or if the discrimination levels were set inappropriately. (Nature Photonics 4 800)

"The only way to recreate the attack was to operate the detector under non-realistic conditions," explained **Shields**. *"In particular, we found that the Trondheim group had included a resistor in the detector circuit that is not necessary and not normally present in a QKD detector. The attack would not work on most QKD systems and it wouldn't work on our system."*

In addition to the redundant resistor, the Shields group found that the detector's discrimination threshold had to be set at an unrealistically high level for the proposed hacking method to work. *"If the output from the detector goes above the discrimination threshold, it registers a detection event,"* said **Shields**. *"Normally, you set the discrimination threshold to be just above the noise level to detect as many of the incident photons as possible. But in order for the blinding attack to work, it has to be set to an artificially high value, making the detector less sensitive. Real QKD systems are not set-up like this."*

About the Author

Jacqueline Hewett is a freelance science and technology journalist based in Bristol, UK.

SOURCE [1]

SOURCE [2]

http://www.ecnmag.com/news/2010/12/toshiba-makes-cryptography-video-breakthrough

Links:
[1] http://www.i-micronews.com/lectureArticle.asp?id=6049
[2] http://www.MDTmag.com/News/Feeds/2010/12/products-electronic-components-toshiba-makes-cryptography-video-breakthrough/