Research promises innovations in secure communications technology

November 20 2014

Dr Zhang Yixin of Nanjing University, China, talks about his development of a true random number generator using only the camera of a smartphone, with no other specialized equipment. To date, true random number generators have required the use of expensive, dedicated auxiliary equipment, and Dr Zhang's innovations may lead to new, widespread applications in secure communications.

How did you come to work in this field?

My major was more related to radio communication as an undergraduate. About eight years ago, I started a PhD at Nanjing University, that was the beginning of my research in optical. In 2011, I joined NTRC at Nanyang Technological University in Singapore as a postdoctoral research fellow. The lab had just begun a joint military project on unconditional encrypted optical communication. That is where my current research work really began. Two years later I returned to Nanjing University as a lecturer and my current main field of research is single photon level optical signal detection and its applications, such as the true random number generator (TRNG) based on photon distribution.

What uses do you have in mind for this?

True random numbers are the key to secure communication, even if quantum technology is included. A TRNG based on an off-the-shelf

image sensor, rather than a thousands-of-dollars photon counter, would be much more attractive for portable personal encryption applications, such as E-payment, privacy call and cryptographic data transmission on a smartphone or laptop. In the near future, the security level of personal devices has to be enhanced with new encryption technology to stand against the technological advances of eavesdroppers; this is the goal of our current project.

What have you reported in your Letter?

Present TRNGs are mainly based on specialised, expensive hardware like single photon detectors, chaotic lasers and radioactive nuclei, which are more suited to commercial or academic applications than personal usage. We present a portable TRNG configuration simply based on the camera of a smartphone. The randomness of the output bit sequence has been proved with NIST tests, and all necessary processing functions could be fully integrated within Android software in the near future.

This approach offers a promising solution for portable personal encryption, since no equipment is needed except the smartphone itself. Back in my PhD days, working on micro-structure imaging, our group confirmed by experiment that in certain conditions, shot noise other than thermal noise can dominate the overall noise characteristics of a high-sensitivity CCD image sensor. Commonly speaking, shot noise of photocurrent is believed to be a quantum process and true random number could be generated accordingly. However, the performance of image sensors on smartphones were not as good then. Two or three years later, I saw a picture taken by my colleague's latest phone, and thought maybe it was time to realise the portable TRNG with smartphone camera.

How do you think the field will develop in the next

decade?

I see two main trends in recent TRNG research. The first is realising higher bit rates; speeds of gigabits per second were reported several years ago. The second is looking for new physical random phenomena that are more reliable. Arguments have always existed on whether chaotic process is as random as quantum process. However, I believe that the integration of TRNGs is very likely to be the main topic in the future. TRNGs are still too big and expensive for most practical applications. Integration of optics and electronics components on a single chip is necessary for portable and low-cost TRNGs. Meanwhile, TRNGs only solve the random number generation problem, a communication protocol which employs true random numbers as secret keys for encryption also needs to be developed.

Where does your work go from here?

Here at the Institute of Optical Communication Engineering at Nanjing, my group will try to improve the Android App for TRNGs to automatically adapt to different types of smartphone, since the camera setting is essential to the overall performance of output random bits. We are also working on high-speed single photon counting technology based on avalanche photodiodes to improve the detection speed if higher rates are required.

Another research area we are involved in is fibre optical sensing, with the goal of locating eavesdroppers in time, while they are intercepting optical signals from fibre communication links. Probe pulse coding based on TRNGs will be used for the improvement of measuring speed, spatial resolution and dynamic range.

More information: "Portable true random number generator for

personal encryption application based on smartphone camera." *Electronics Letters*, Volume 50, Issue 24, 20 November 2014, p. 1841 – 1843 DOI: 10.1049/el.2014.2870 , Print ISSN 0013-5194, Online ISSN 1350-911X