The quest for true randomness and uncrackable codes

May 22 2014, by Senne Starckx

Quantum cryptography is said to be uncrackable. It will stay safe, but only if true randomness, the generation and use of intrinsically random numbers, can be achieved.

Each time we read our e-mail, login to online shopping sites, watch a movie online or use our mobile phone, we are using random numbers to establish a secure connection. Randomness is a crucial ingredient in practically every area of information processing. And, most importantly, in cryptography. But because all conventional computing processes are based on classical physics, looking for true randomness is like searching

for the pot of gold at the end of the rainbow. This explains why even the most sophisticated present-day encryption systems can fall prey to hackers.

Enter quantum computing. Incorporating the inherent random nature of the quantum world in a computer yields a revolutionary new way of producing true random numbers. Thanks to this, real uncrackable codes are in sight. The EU funded project RAQUEL, started in October 2013, evaluates the role played by randomness in quantum information processing. Project coordinator Jan Bouda, a researcher in Informatics at Masaryk University in Brno, in the Czech Republic, talks to youris.com why true randomness is so important and what it will mean for cryptography.

Why can my computer not produce true random numbers?

Conventional computing is based on classical physical principles. And in classical physics, there is not a single process that is intrinsically random. Hence, the randomness generated by classical devices, like your PC, is rather a consequence of our ignorance of the initial setup. On the contrary, randomness obtained from quantum computers is true, as the measurement is supposed to be intrinsically random. (ironically) That is if quantum physics is right.

So why is randomness so important?

Randomness is used in a huge number of efficient algorithms. In fact, for many problems, algorithms using random choices are far more efficient than the best-known deterministic algorithms. These algorithms are used to reduce the amount of communication for distributed computation, such as, in cloud computing, and more importantly, for

cryptography. Any application that should work securely needs random numbers.

On the other hand, to produce high-quality random numbers is not easy. Even in specialised devices, like in quantum random number generators, the amount of random numbers you can produce per second is strictly limited. Random numbers are important in all areas of computer science. But in cryptography the quality is a deal breaker. In many applications, even a minor flaw in randomness can completely jeopardise the security.

What are your current research goals?

The overall goal is to establish the role of randomness in quantum information processing. We focus on two basic aspects. How to produce true randomness efficiently. And how to use this randomness in an efficient way, so that the produced randomness is not wasted.

Can you name some possible, practical applications of the research?

I guess that the first applications will be in securing high-importance communication links, like between the headquarters of banks and their branches or between different government institutions. These technologies have already been available for many years and are being deployed. A good example is the SECOQC project, in which several big firms in Europe use quantum cryptography to secure their internal communication and avoid espionage from the outside world. Another example is ID Quantique, a Swiss firm that sells so-called quantum key distributors. These are devices that already produce random numbers based on quantum physics.