Using entangled particles to create unbreakable encryption

May 30 2024, by Rahel Collyer-Hoar

Prof. Ekert explains the fundamental concepts of randomness and quantum cryptography. Credit: Tomomi Okubo/OIST

The discovery of quantum mechanics opened the door to fundamentally new ways of communicating, processing, and protecting data. With a

quantum revolution well underway, long unimaginable opportunities are coming within our reach.

From the fundamental questions on how the universe works to secure communication—it is quantum mechanics that holds our future's solutions. Professor Artur Ekert, pioneer in the field and father of quantum cryptography, has been Professor (Adjunct) and the head of OIST's Quantum Information Security Unit since April 2021. Professor Ekert, who is now able to stay more frequently at OIST after the pandemic, was interviewed.

With a background in applied mathematics, he had not planned to work in physics until stumbling upon "The Feynman Lectures on Physics" in a library—"I read it and was completely hooked!" Prof. Ekert says. With this newly found passion, he began working towards his Ph.D. at the University of Oxford, where he also met his mentor David Deutsch, the pioneer of quantum computation. At the same time, he came across another influential paper on quantum entanglement, written by the famous physicist Alain Aspect.

"I was deeply impressed—the paper showed that quantum mechanics is inherently unpredictable. This was my starting point when I understood that this can be used for secure communications," says Prof. Ekert. But before these groundbreaking experiments of Aspect and colleagues, there was fierce debate about whether experiments in quantum mechanics are inherently unpredictable or not.

While it was possible to get statistical predictions about the outcomes of these experiments, determinate statements always remained out of reach. "Now the question was, do we deal with true randomness in quantum mechanics or just our inability to yet predict outcomes well enough?" explains Prof. Ekert. It turned out that the answer to this question also held the key to the development of quantum cryptography.

Is there true randomness in the universe?

Random events can be categorized into two different types, which scientists refer to as objective and subjective randomness. "For example, something might appear random to you but not to me because I have more information that allows me to understand and predict the event. If you don't have access to this additional information the event will appear random to you—this is what we call subjective randomness," explains Prof. Ekert.

Surprisingly, the classical example of a coin toss belongs to the category of subjective randomness. With enough knowledge about the initial conditions, the coins' movement and structure, the air circulation in the room and more, the result of any coin toss would become perfectly predictable. "Objective randomness on the other hand is an event for which you cannot predict the outcome even if you knew absolutely everything about it," Prof. Ekert says.

Whether quantum physics has elements of this objective randomness was debated among scientists in the 20th century and got some very prominent opposition from Albert Einstein.

"He thought that we can't predict the outcomes of experiments in quantum mechanics because we lack information, not because they are inherently unpredictable," Prof. Ekert says. If that were correct and those missing pieces of information could be identified, the outcome of experiments in quantum mechanics should have become predictable. "He called this missing information hidden variables," explains Prof. Ekert.

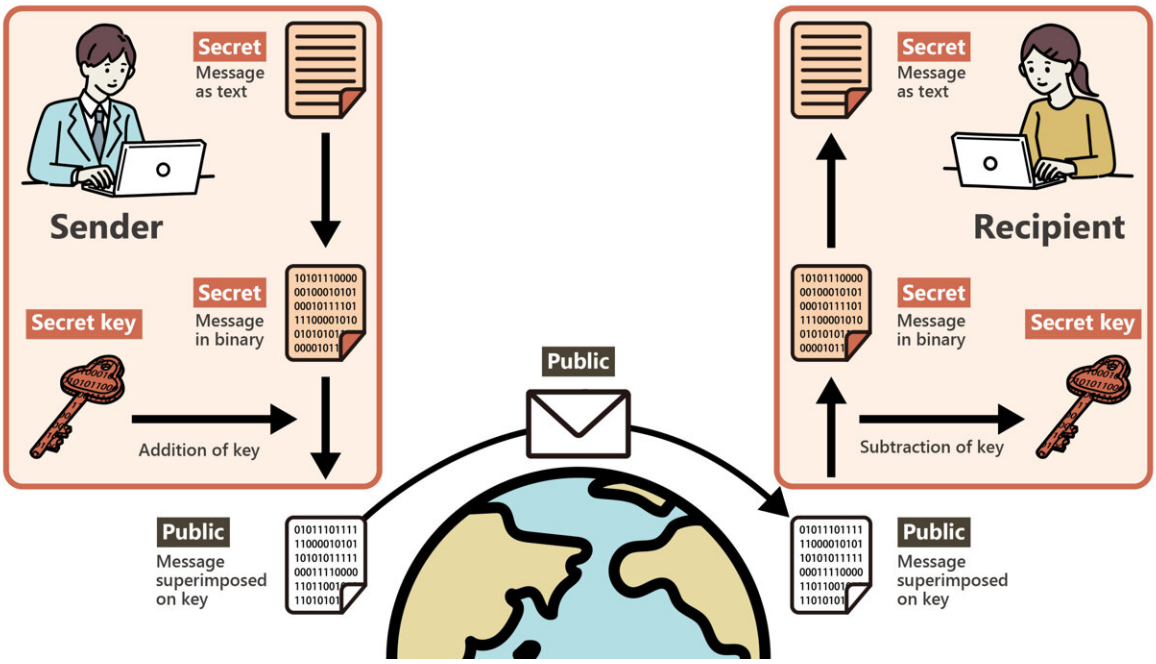
This theoretical debate raged on for roughly 30 years, until scientist John Bell came up with a testable hypothesis, now also referred to as Bell's inequality. This test, among other uses, made it possible to answer the

question if quantum events are truly random or not.

This is how it works in a nutshell; during a suitable experiment using entangled photons a specific parameter is measured. If this parameter is outside an expected range, it supports that events on a quantum level have an objectively random component, but if it falls within the expected range, then Einstein's objections are correct and there are hidden variables.

"The problem was that when Bell published his work, it wasn't yet possible to perform these highly complicated experiments," says Prof. Ekert. With the math but not the technical means to perform the test, the debate remained unanswered for another decade. Until the 1970s, when these experiments finally became possible, John Clauser was among the first to perform them.

"When he does these first experiments, he observes a violation of Bell's inequality which supported the fact that nature at its foundation is random," Prof. Ekert says.



Confidential information is translated into binary before being superimposed onto a secret random encryption key by performing binary addition. The result is another random sequence of ones and zeros. Because this sequence is also random, nobody can find the confidential information hidden in it, even when analyzing the sequence. At this stage, the messages, also called cryptograms, can only be decoded with the matching key. That makes it possible to send the message safely even when using non-encrypted or public methods. Once the recipient gets the cryptogram, they can recover the confidential information hidden by subtracting the random sequence of the encryption key. Credit: : Kaori Serakaki/OIST

But with the still limited technology of the time, this exciting finding remained preliminary at first. In fact, certainty on the matter was not reached until the late 90s. Among others, it was the groundbreaking work of Alain Aspect, Nicolas Gisin, Ronald Hanson, Jianwei Pan and Anton Zeilinger, on the nature of quantum entanglement and the Bell inequalities, that confirmed the fundamental workings of quantum

mechanics for good—showing that there is true randomness in quantum events.

In 2022 Aspect, Clauser and Zeilinger shared a Nobel prize for their pioneering experimental efforts.

From quantum mechanics to quantum cryptography

Upon learning about all this while working towards his Ph.D., Prof. Ekert realized that randomness can be used to create a way to develop unbreakable encryption. Before secure communications went quantum, cryptography had already made it possible to transmit information safely, except for one crucial pitfall.

"Let's imagine you want to transmit information safely to another person. In that case, both of you need something called a cryptographic key—which is a completely random sequence of ones and zeros. This key needs to be kept strictly secret!" says Prof. Ekert. While the key is random and therefore meaningless, it will later allow its holder to decode the sent message.

But this traditional method of encryption has a major safety obstacle: Keeping the key secret. Should access be gained unauthorized, any messages sent could be decoded and how could there ever be complete certainty that nobody had gained access to the secret keys?

Classically, this problem was addressed by using protected lines for communication and through the work of cybersecurity specialists implementing various safety features to protect encryption keys.

"But you see, even with the best security in place, you could never be 100% sure that nobody had gotten access," Prof. Ekert points out.

All this changed when the experiments on Bell's inequality showed that quantum mechanics has an inherently random component. "A solution is to use quantum keys. These are generated using entangled photons," Prof. Ekert explains.

This method of generating a cryptographic key makes it possible to test if anyone has had unauthorized access by using Bell's theorem. "If your key violates Bell's inequalities, you can be sure nobody had access to your key," Prof. Ekert says. With this, he had discovered an entirely novel way of securing communication: Quantum cryptography.

This encryption method is now more important than ever, as progress in the development of quantum computers will make classical encryption less safe—a problem for sensitive data, for example in the medical or financial sector. Here quantum cryptography offers a way to ensure protection, but it won't likely become the standard for all communication.

"Quantum cryptography will not completely replace classical methods, because there is not always a need for perfect security. Not every car needs to be up to Formula One standards—it is the same for encryption," Prof. Ekert says.

Nevertheless, developing modern cybersecurity strategies that keep up with today's complex technological world is a key challenge for science and society alike, and one of the reasons that brought Prof. Ekert to OIST.

"I am here to help create a vibrant quantum and cyber security community in Okinawa and I also want to help educate people about cybersecurity and improve data protection," says Prof. Ekert.

A second focus will be his research on the concept of randomness, for

which OIST offers ideal conditions. "I appreciate the nice and quiet environment in Okinawa," Prof. Ekert points out. While it is now a fact that objective randomness plays a role in quantum mechanics, Prof. Ekert's research here at OIST tackles a maybe comparatively fundamental question about the nature of our universe: "I am interested in why things are random," he says.

Provided by Okinawa Institute of Science and Technology