'Unbreakable' security codes inspired by nature

April 4 2014

A revolutionary new method of encrypting confidential information has been patented by scientists at Lancaster University.

They have been inspired by their discoveries from human biology, which model how the heart and lungs coordinate their rhythms by passing information between each other.

A mathematical model based on the complex interaction between these organs has now been transferred to the world of modern communications.

This discovery could transform daily life which is reliant on secure electronic communications for everything from mobiles to sensor networks and the internet.

Every device, from your car key to online bank account, contains different identification codes enabling information to be transferred in confidence. But the race to outwit the hackers means there is a continual demand for better encryption methods.

Inspiration for the new method of encryption came from interdisciplinary research in the Physics Department (www.physics.lancs.ac.uk/resear … d-biomedical-physics) by Dr Tomislav Stankovski, Professor Peter McClintock, and Professor Aneta Stefanovska, and the patent includes Dr Robert Young.

Professor McClintock commented that this is a significant discovery.

He said: "This promises an encryption scheme that is so nearly unbreakable that it will be equally unwelcome to internet criminals and official eavesdroppers."

Professor Stefanovska emphasized the interdisciplinary aspect: "As so often happens with important breakthroughs, this discovery was made right on the boundary between two different subjects – because we were applying physics to biology."

Dr Stankovski said: "Here we offer a novel encryption scheme derived from biology, radically different from any earlier procedure. Inspired by the time-varying nature of the cardio-respiratory coupling functions

recently discovered in humans, we propose a new encryption scheme that is highly resistant to conventional methods of attack."

The advantage of this discovery is that it offers an infinite number of choices for the secret encryption key shared between the sender and receiver. This makes it virtually impossible for hackers and eavesdroppers to crack the code.

The new method is exceptionally resistant to interference from the random fluctuations or "noise" which affects all communications systems.

It can also transmit several different information streams simultaneously, enabling all the digital devices in the home, for example, to operate on one encryption key instead of dozens of different ones.

More information: Tomislav Stankovski, Peter V. E. McClintock, and Aneta Stefanovska , "Coupling Functions Enable Secure Communications," American Physical Society's journal *Physical Review X*, journals.aps.org/prx/abstract/ … 03/PhysRevX.4.011026

Provided by Lancaster University