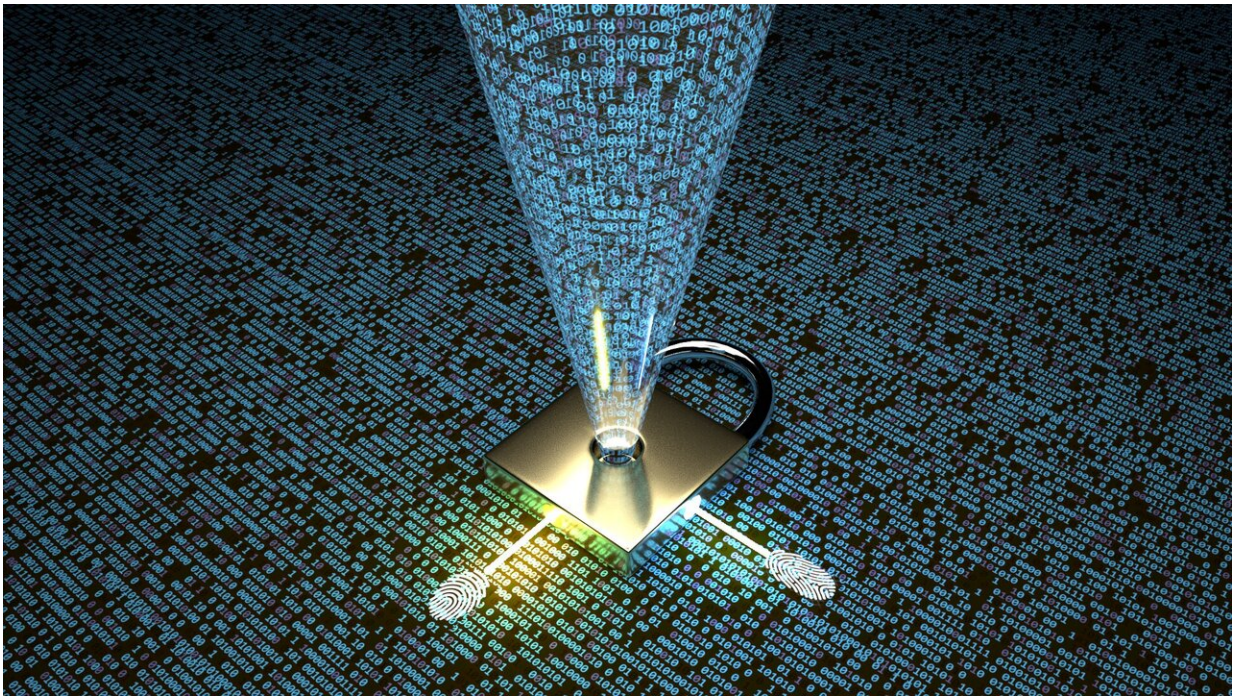
New security system to revolutionize communications privacy

December 20 2019



A new uncrackable security system created by researchers at the University of St Andrews, King Abdullah University of Science and Technology (KAUST) and Center for Unconventional Processes of Sciences (CUP Sciences) is set to revolutionize communications privacy. Credit: KAUST

A new, uncrackable security system created by researchers at King Abdullah University of Science and Technology (KAUST), the University of St Andrews and the Center for Unconventional Processes

of Sciences (CUP Sciences) is set to revolutionize communications privacy.

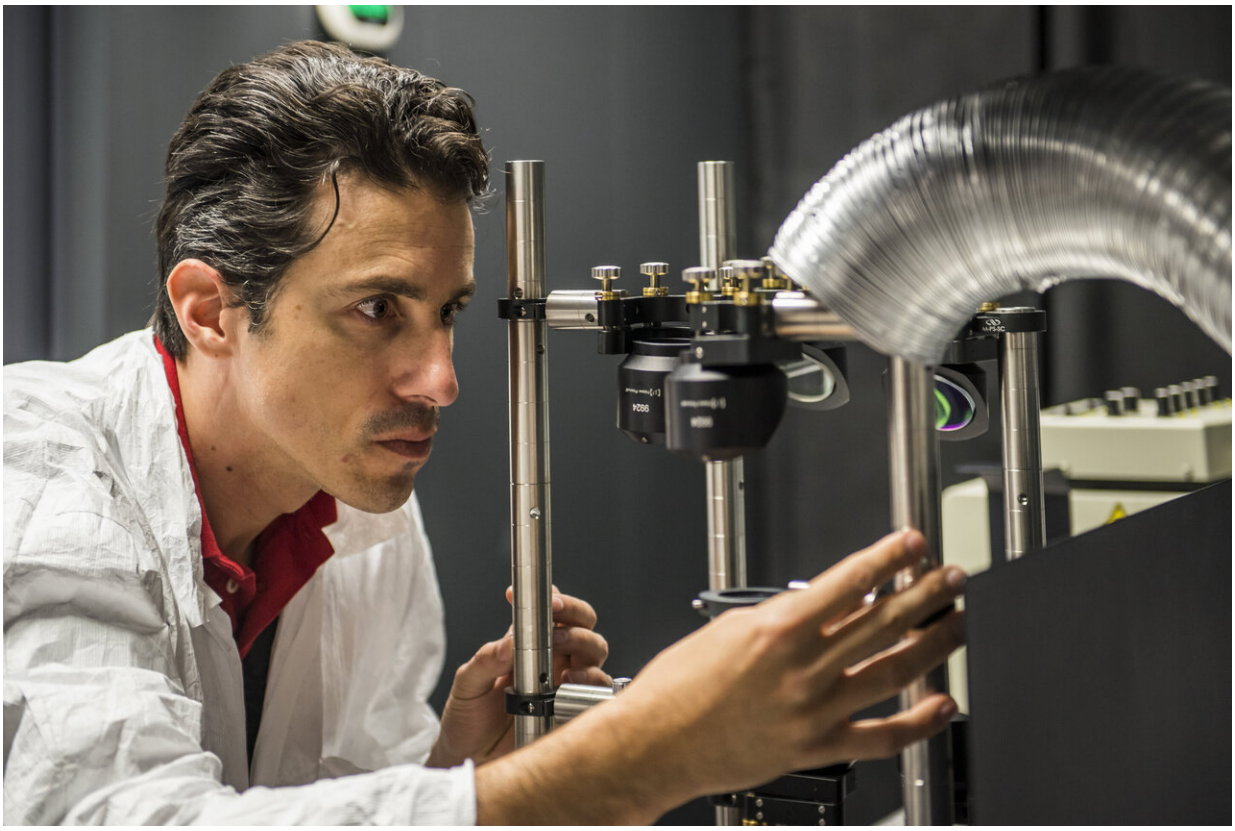
The international team of scientists have created optical chips that enable information to be sent from user to user using a one-time un-hackable communication that achieves "perfect secrecy" allowing confidential data to be protected more securely than ever before on public classical communication channels.

Their proposed system uses silicon chips that contain complex structures that are irreversibly changed, to send information in a one-time key that can never be recreated nor intercepted by an attacker.

The results published in the scientific journal *Nature Communications* open a new pathway towards implementing perfect secrecy cryptography at the global scale with contained costs.

"This new technique is absolutely unbreakable, as we rigorously demonstrated in our article. It can be used to protect the confidentiality of communications exchanged by users separated by any distance, at an ultrafast speed close to the light limit and in inexpensive and electronic compatible optical chips," says Professor Andrea di Falco of the School of Physics and Astronomy at the University of St. Andrews and first author of the study.

Current standard cryptographic techniques allow information to be sent quickly but can be broken by future computers and quantum algorithms. The research team say their new method for encrypting data, is unbreakable, and uses the existing communication networks, taking up less space on the networks than traditional encrypted communications.



A new uncrackable security system created by researchers at the University of St Andrews, King Abdullah University of Science and Technology (KAUST) and Center for Unconventional Processes of Sciences (CUP Sciences) is set to revolutionize communications privacy. Credit: KAUST

"With the advent of more powerful and quantum computers, all current encryptions will be broken in very short time, exposing the privacy of our present and, more importantly, past communications. For instance, an attacker can store an encrypted message that is sent today and wait for the right technology to become available to decipher the communication," says Dr. Andrea Fratalocchi, Associate Professor of Electrical Engineering at KAUST and co-author of the study.

"Implementing massive and affordable resources of global security is a

worldwide problem that this research has the potential to solve for everyone, and everywhere. If this scheme could be implemented globally, crypto-hackers will have to look for another job," Dr. Fratalocchi continues.

The new method uses the classical law of physics to protect the messages and in particular the second law of thermodynamics. The technique achieves perfect secrecy, meaning a hacker will never be able to access the information contained in the communication.

Keys generated by the chip, which unlock each message, are never stored and are not communicated with the message, nor can they ever be recreated, even by the users themselves, adding extra security.

"This system is the practical solution the cybersecurity sector has been waiting for since the perfect secrecy theoretical proof in 1917 by Gilbert Vernam. It'll be a key candidate to solving global cybersecurity threats, from private to national security, all the way to smart energy grids." says Dr. Aluizio M Cruz, co-founder and CEO of the Center for Unconventional Processes of Sciences (CUP Sciences) in California, and co-author of the study.

The team is currently working on developing commercial applications of this patented technology, have a fully functional demo and are building user-friendly software for this system.

More information: Di Falco, A., Mazzone, V., Cruz, A. & Fratalocchi A. Perfect secrecy cryptography via correlated mixing of chaotic waves in irreversible time-varying silicon chips. *Nature Communications*, (2019). DOI: 10.1038/s41467-019-13740-y