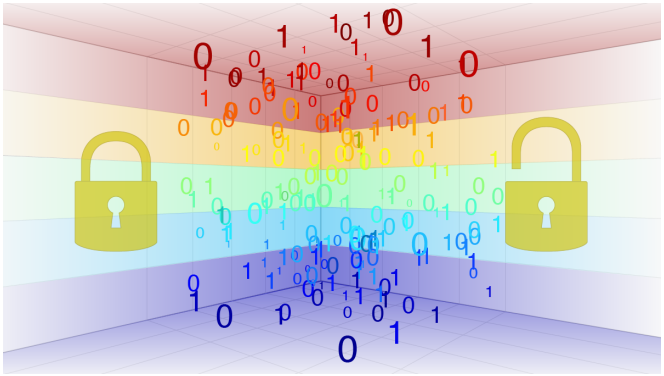
Researchers prove the security of the Vector Stream Cipher

17 July 2017



Kyoto University demonstrates the security of a cipher based on chaos theory. Credit: Kyoto Univeristy / Eiri Ono

How do we know if the electronic keys we use in our devices are really secure? While it is possible to rigorously test the strength of a cipher—a kind of digital data lock—there are rarely any definitive proofs of unbreakability. Ciphers are highly complex, and while they may ward off certain attacks, they might be vulnerable to others.

Now, in a series of papers published in *IEEE Transactions on Information Forensics and Security* and *IEICE Nonlinear Theory and Its Applications*, researchers from Kyoto University have definitively demonstrated the strength of a cipher based on principles of chaos theory.

The group's Vector Stream Cipher (VSC) is the first example of a 128-bit key chaotic cipher with provable security. "We first developed VSC in 2004 as a simple, fast cipher, and parts of it have already been utilized in the private sector," explains Ken Umeno, leader of the study. "Many theoretical attacks in the past have failed to break it, but until now, we hadn't shown definitive proof of security."

The researchers conducted a number of tests, such as a method to evaluate the lock's randomness. Many ciphers rely on number sequences that appear to be random, but are actually generated through recurring relations that are vulnerable to being reproduced.

"Before evaluating the security of VSC with randomness tests, we found a way to make it significantly more reliable and sensitive," continues Umeno. "We then continued this refinement during the actual investigation."

The research highlights that VSC is not only secure, but structurally simple and low on memory usage compared with existing technology, making it useful for high-density data transmission applications such as in 5G mobile networks and 4K television broadcasts.

Umeno concludes, "Chaotic ciphers have been in use for about 30 years, but before this study we had not expected to find proof of security. We hope that our work will be studied widely and applied throughout our digital world."

More information: "Further improving security of Vector Stream Cipher" *Nonlinear Theory and Its Applications, IEICE*, DOI: 10.1587/nolta.2.1101

Provided by Kyoto University