ASIAN SCIENTIST

July 25, 2017 Technology By **Asian Scientist Newsroom**

Chaos Theory Strengthens Digital Locks

Japanese researchers report definitive proof of invulnerability for a digital lock based on the principles of chaos theory.

AsianScientist (July 25, 2017) – Using the principles of chaos theory, researchers from Kyoto University have definitively demonstrated the strength of a 128-bit digital lock for cybersecurity applications. Their findings are published in the journal *Nonlinear Theory and Its Applications*.

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 invulnerability. Ciphers are highly complex, and while they may ward off certain attacks, they might be overcome by others.

In this study, the group led by Professor Ken Umeno of Kyoto University released new data on its Vector Stream Cipher (VSC), 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," explained Umeno. "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," Umeno added. "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.

> "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," said Umeno.

The article can be found at: Iwasaki & Umeno (2017) Further Improving Security of Vector Stream Cipher.

———

Source: Kyoto University; Photo: Shutterstock.

Disclaimer: This article does not necessarily reflect the views of AsianScientist or its staff.

#Algorithm #Computer Science #Cybersecurity #Japan #Kyoto University