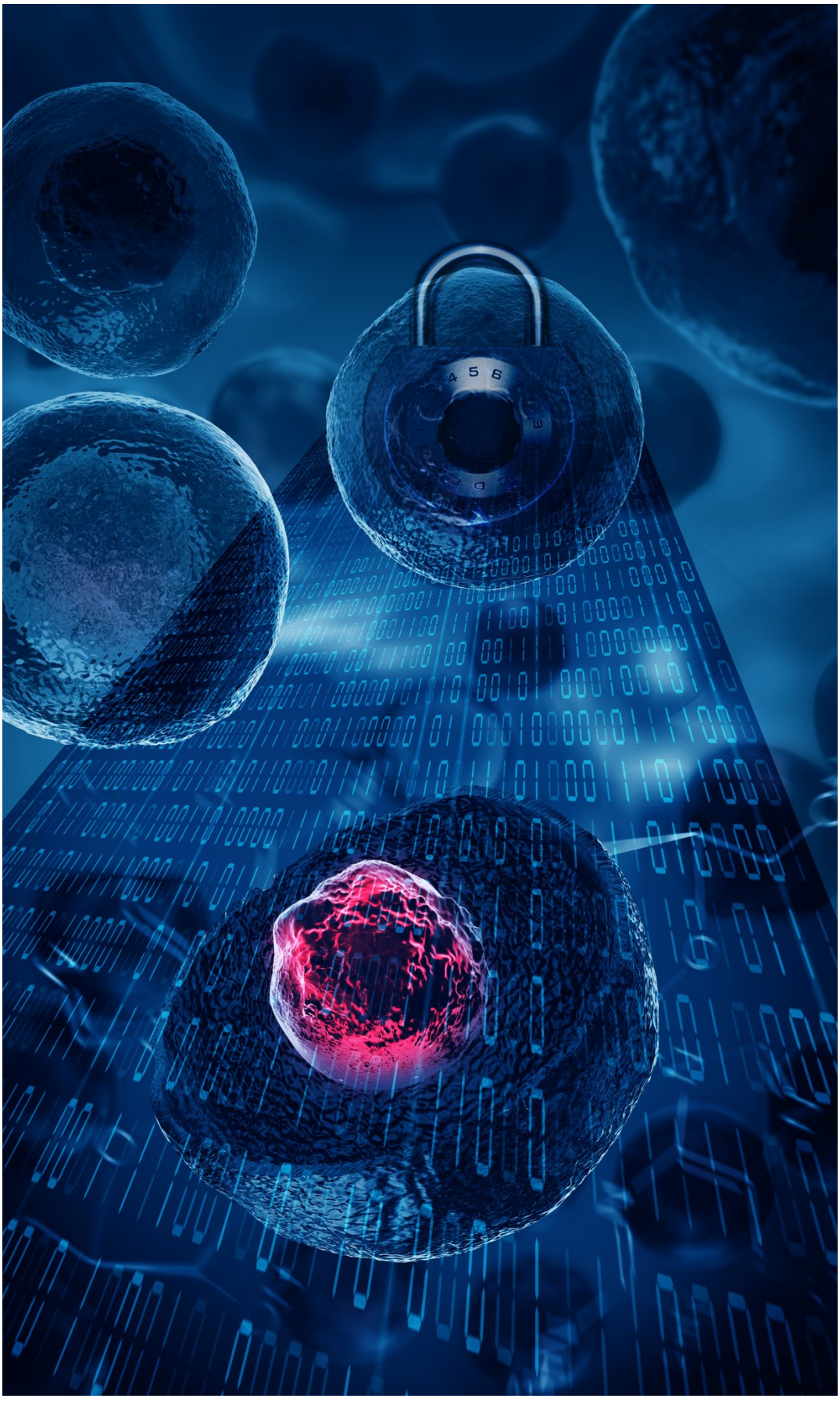
Better security achieved with randomly generating biological encryption keys

December 19 2018



Living cells, regardless of the type, can be kept around for a long time and because they move constantly, can be photographed repeatedly to create new encryption keys Credit: Jennifer M. McCann / Penn State MRI

Data breaches, hacked systems and hostage malware are frequently topics of evening news casts—including stories of department store, hospital, government and bank data leaking into unsavory hands—but now a team of engineers has an encryption key approach that is unclonable and not reverse-engineerable, protecting information even as computers become faster and nimbler.

"Currently, encryption is done with mathematical algorithms that are called one-way functions," said Saptarshi Das, assistant professor of engineering science and mechanics, Penn State. "These are easy to create in one direction, but very difficult to do in the opposite direction."

An example of this is multiplying two prime numbers. Assuming the original numbers are very large, reverse engineering from the result becomes very time and computer-resource heavy.

"However, now that computers are becoming more powerful and quantum computing is on the horizon, using encryption that relies on its effectiveness because it is monumentally time consuming to decrypt won't fly anymore," Das said.

Only truly random encryption keys are unclonable and not capable of being reverse-engineered because there is no pattern or formula in the process. Even so-called random number generators are really pseudo-random number generators.

"We need to go back to nature and identify real random things," said Das. "Because there is no mathematical basis for many biological processes, no computer can unravel them."

The researchers, who also included Akhil Dodda, graduate student in engineering science and mechanics; Akshay Wali, graduate student in electrical engineering; and Yang Wu, postdoctoral fellow in engineering science and mechanics, looked at human T cells. They photographed a random, 2-dimensional array of T cells in solution and then digitized the image by creating pixels on the image and making the T cell pixels "ones" and the empty spaces "zeros."

"When we started there were a few papers out using nanomaterials," said Dodda. "However, they weather (nanomaterials) out of the material and are stationary."

Living cells, regardless of the type, can be kept around for a long time and because they move constantly, can be photographed repeatedly to create new encryption keys.

"We need a lot of keys because the population of the world is 7 billion," said Das. "Each person will generate a megabyte of data every second by 2020."

Besides encryption keys for personal computers, the keys are also needed for medical, financial and business data, and much more. If something is hacked or malfunctions, this method would also allow rapid replacement of the encryption key.

"It is very difficult to reverse-engineer these systems," said Dodda. "Not being able to reverse-engineer these keys is an area of strength."

The researchers are currently using 2,000 T cells per encryption key. The

team reports in a recent issue of *Advanced Theory and Simulations* that even if someone knows the key generation mechanism, including cell type, cell density, key generation rate and key sampling instance, it is impossible for anyone to breach the system. It is simply not possible from that information to bust the encryption.

"We need something secure, and biological species-encrypted security systems will keep our data safe and secure everywhere and anytime," said Wali.

More information: Akhil Dodda et al, Biological One-Way Functions for Secure Key Generation, *Advanced Theory and Simulations* (2018). DOI: 10.1002/adts.201800154

Provided by Pennsylvania State University

Citation: Better security achieved with randomly generating biological encryption keys (2018, December 19) retrieved 23 July 2024 from https://phys.org/news/2018-12-randomly-biological-encryption-keys.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.