World-first program to stop hacking by supercomputers

July 19 2018

IT experts at Monash University have devised the world's leading post-quantum secure privacy-preserving algorithm – so powerful it can thwart attacks from supercomputers of the future.

The Lattice-Based One Time Ring Signature (L2RS) enhanced security and privacy-preserving features enable large transactions and transfer of data without risk of being hacked by quantum computers and privacy revoked by unauthorised users.

Monash IT experts consider L2RS as a significant leap forward in maintaining data security, user privacy and integrity for blockchain technology as the race to build powerful quantum computers gains momentum.

Senior Lecturer and Director of the Blockchain Research Lab at Monash, Dr. Joseph Liu, says data security will become essential as quantum computing gets closer to being able to unravel the technology that underpins the security of blockchains—a milestone estimated to reach the world within the next 10 years.

"The L2RS deploys cryptographical techniques to protect the privacy of users. It allows any user to hide his identity among a group of users. The transaction amount will be hidden as well. No one knows how much money has been transferred in each transaction," Dr. Liu said.

"It is also post-quantum secure. That is, even in the existence of the

future powerful quantum computer—which can easily break the current security algorithms such as RSA—HCash is still secure, and user privacy remains preserved," he said.

Dr. Liu said blockchain has legitimate potential to change the world to create new foundations for economic and social systems, and a working quantum computer could, in theory, break today's cryptography.

"Therefore, HCash has a significant advantage over other cryptocurrency exchanges even after the practical rise of quantum computers," he said.

The L2RS algorithm was announced at the 23rd Australasian Conference on Information Security and Privacy.

Provided by Monash University

Citation: World-first program to stop hacking by supercomputers (2018, July 19) retrieved 31 January 2023 from https://phys.org/news/2018-07-world-first-hacking-supercomputers.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.