PHYS.ORG

Towards equal access to digital coins

February 8 2017

Scientists at the Interdisciplinary Centre for Security, Reliability and Trust (SnT) of the University of Luxembourg have developed an important mathematical algorithm called "Equihash." Equihash is a core component for the new cryptocurrency Zcash, which offers more privacy and equality than the famous Bitcoin. Zcash came into operation as an experimental technology for a community-driven digital currency in late 2016.

Bitcoin is by far the most recognized and widely used digital currency. It was introduced in January 2009 and has garnered much attention since then. But it is not the only one of its kind. Wikipedia lists nearly one hundred cryptocurrencies boasting more than 1 million US dollar market capitalisation.

One of the newest cryptocurrencies is "Zcash," which can be seen as an update to the Bitcoin protocols. In Bitcoin, the transfer of coins is recorded in a global ledger, the so-called blockchain. The validity of the latest transfers in the blockchain is verified about every ten minutes. Verifying the transfers and creating new blocks for the blockchain (the so-called mining) requires a lot of computing power, which is provided by distributed computers worldwide. The "miners" who allocate the processing power are rewarded with new coins.

Zcash is trying to resolve two main shortcomings of Bitcoin: its lack of privacy for transactions and the centralization of transaction verification into the hands of a mere dozen miners who have invested in large amounts of specialized mining hardware: Bitcoin is prone to such centralization because the computational load of the bitcoin mining algorithm can be split into many different small tasks, which can be conducted in parallel. The algorithm is easy to implement in dedicated, energy-efficient and cheap microchips, but not suited to standard hardware. Bitcoin mining today is therefore done on special-purpose supercomputers which are located in places with cheap electricity and/or cheap cooling. Such supercomputers are expensive, costing millions of euros, but provide much more mining power than if one were to use standard PC hardware of the same price.

Prof. Alex Biryukov, head of the research group "Cryptolux" and Dr. Dmitry Khovratovich at SnT have developed the algorithm "Equihash" which can resolve this problem. Equihash is a so called memory-hard problem, which can not be split up into smaller working packages. It can be more efficiently calculated on desktop-class computers with their multiple processing cores and gigabytes of memory than on special hardware chips. "If 10.000 miners with a single PC were active, in Zcash the investment to compete with them would be 10.000 times the price of a PC, while with bitcoin, the investment would be significantly smaller," says Khovratovich. This creates a more democratic digital currency by allowing more users to contribute to the mining process. Khovratovich adds: "The strength of a cryptocurrency comes from the fact that the ledger is globally distributed. Our Equihash algorithm reverses the situation back to this more ideal world."

Equihash was first presented at the Network and Distributed System Security Symposium last year – one of the top-5 IT security events. Prof. Biryukov comments: "Since Equihash is based on a fundamental computer science problem, advances in Equihash mining algorithms will benefit computer science in general. Equihash is so far unique among all the mining algorithms: it is memory-hard on the one hand and very easy to verify on the other." In other words, while mining new coins with Zcash/Equihash is comparatively expensive, hence posing a smaller risk of monopolization because it requires large amounts of computer memory and hard computational work, checking that the new coins are genuine is memoryless, fast and cheap.

Understanding these advantages, the creators of Zcash chose Equihash as the algorithm for mining coins and verifying transfers. Equihash itself is not limited to use in Zcash and can be used in any cryptocurrency, including Bitcoin.

"With our contribution to Zcash, the Cryptography and Security lab (CryptoLux) has shown its strength in innovative research that has immediate applications in the financial technology industry," says SnT´s director, Prof. Björn Ottersten. "We invite students to follow us in this promising field," adds Professor Biryukov: "There are still lots of challenging research problems to solve."

More information: Equihash: Asymmetric proof-of-work based on the Generalized Birthday problem. hdl.handle.net/10993/22277

Provided by University of Luxembourg

Citation: Towards equal access to digital coins (2017, February 8) retrieved 18 April 2024 from https://phys.org/news/2017-02-equal-access-digital-coins.html