北京大学前沿计算研究中心
Center on Frontiers of Computing Studies, Peking University

静园5号院
前 沿 讲 座

Mutator Set: a Scalable Cryptographically Authenticated Data Structure for Private UTXOs

Dr. Alan Szepieniec

Co-founder & Chief Architect
Neptune

Host: 刘天任 助理教授
2023年11月17日 星期五 16:00
静园五院204室

Abstract

A mutator set is a cryptographic data structure for efficiently authenticating operations on large sets, similar to a Merkle tree but with new features:

- you can add items to the set;
- you can remove items from the set;
- you cannot link additions to removals.

Depending on your perspective, it is a) a succinct decoy-and-nullifier set such as used in ZCash and Monero (but without an ever-expanding nullifier set); b) a cryptographic accumulator scheme with unlinkable set updates; or c) a mixnet without operators. In the context of cryptocurrencies, mutator sets are capable of concealing the links between transaction outputs and inputs without sacrificing scalability.

Biography

Dr. Alan Szepieniec obtained his PhD from KU Leuven, Belgium, in 2018, on the topic of post-quantum cryptography. After that he pivoted towards hash function design and interactive proof systems in the capacity of researcher for various blockchain foundations. Since 2022 he has been working as co-founder and chief architect of the Neptune cryptocurrency (https://neptune.cash/) which uses Mutator Sets to succinctly represent the UTXO set.

扫下方二维码
观看讲座直播

http: //cfcs.pku.edu.cn/