A Secure Multi-party Computation Protocol Combines Pederson Commitment with Schnorr Signature for Blockchain

Title	A Secure Multi-party Computation Protocol Combines Pederson Commitment with Schnorr Signature for Blockchain
Publication Type	Conference Paper
Year of Publication	2020
Authors	Feng, Liu, Jie, Yang, Deli, Kong, Jiayin, Qi
Conference Name	2020 IEEE 20th International Conference on Communication Technology (ICCT)
Date Published	Oct. 2020
Publisher	IEEE
ISBN Number	978-1-7281-8141-7
Keywords	anonymous messaging, blockchain, contracts, data privacy, Electronic mail, privacy, privacy computing, Protocols, pubcrawl, Public key, resilience, Resiliency, secure multi-party computation, zero-knowledge proof

Abstract

Blockchain is being pursued by a growing number of people with its characteristics of openness, transparency, and decentralization. At the same time, how to secure privacy protection in such an open and transparent ledger is an urgent issue to be solved for deep study. Therefore, this paper proposes a protocol based on Secure multi-party computation, which can merge and sign different transaction messages under the anonymous condition by using Pedersen commitment and Schnorr Signature. Through the rationality proof and security analysis, this paper demonstrates the private transaction is safe under the semi-honest model. And its computational cost is less than the equivalent multi-signature model. The research has made some innovative contributions to the privacy computing theory.

URL https://ieeexplore.ieee.org/document/9295819

DOI 10.1109/ICCT50939.2020.9295819

Citation Key feng_secure_2020

anonymous messaging blockchain contracts data privacy Electronic mail privacy privacy computing Protocols pubcrawl Public key resilience Resiliency secure multi-party computation zero-knowledge proof