Sedicii Announces European Patent Grant “Secure Multiparty Computation without Online Communication”

Sedicii's Nil Message Compute protocol granted a European patent.

Sedicii

WATERFORD, IRELAND, June 20, 2024 /EINPresswire.com/ -- Sedicii is delighted to announce that the European Patent Office has awarded it a patent for its secure multiparty computation protocol titled “Secure Multi-Party Computations Without Online Communication”.

Secure Multiparty Computation (SMPC) is a cryptographic protocol that distributes an algorithm across multiple parties where no individual party can see the other parties’ data. It was developed with the primary objective of achieving secure computation between distributed nodes in a network. The parties agree on the function to be computed, and then follow the SMPC protocol to collaboratively compute the output without revealing their secret inputs.

> “This was a critical step forward in bringing secure and private collaborative computation to the internet. I want to congratulate the whole Sedicii team that was involved in this innovation effort.”
>
> *Rob Leslie*

Sedicii’s Nil Message Compute protocol - Secure Multiparty Computations Without Online Communication - moves the state of the art forward for SMPC protocols by combining two cryptographic primitives in a multi-node network to enable Information Theoretic Secure processing of data (i.e. Quantum Safe). The resultant new type of network makes it possible to perform arbitrary, verifiable, decentralized computations at regular CPU speeds without requiring inter-node messaging. This is the breakthrough Sedicii innovation which enables the massive improvements in processing speed over traditional SMPC protocols. The SMPC Protocol enables the creation of a decentralised network of computer nodes that can process data at almost client server speeds without any node sharing its information with any of the other nodes in the network.

Commenting on the patent award, Sedicii's CEO and Founder, Rob Leslie stated that this was a critical step forward in bringing secure and private collaborative computation to the internet and that he wanted to congratulate the whole Sedicii team who have worked so hard over the last number of years to deliver this innovation. Specifically referring to the protocol, he added "the scalability problems associated with SMPC originate from communication between the nodes which is very time-consuming. To address this, the Sedicii protocol combines two cryptographic primitives, One-Time Masking (OTM) and Linear Secret Sharing (LSS). By combining these two cryptographic primitives, the Nil Message Compute protocol removes the need for the network nodes to exchange any messages to perform a computation, avoiding SMPC's scalability problem. Specifically, the OTM does not need to be designed to operate in the presence of active adversaries as this feature is provided by the other cryptographic primitive, LSS. Therefore, there is more freedom for the design of the OTM, which is used to eliminate the need for inter-node communication during the computation step. This has very important practical consequences as it increases the performance to CPU speed and also allows for consensus to be reached between the network nodes without lots of inter-node communication, while also exhibiting best-in-class security."

Rob Leslie
Sedicii
+353 51 302 191
email us here
Visit us on social media:
X
LinkedIn
