An overview of secure multiparty computation and its application to digital asset custody

Matt O'Grady

Technical Report

RHUL–ISG–2022–8

11 April 2022

Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom

Executive Summary

Secure multiparty computation (MPC) as a subfield of cryptography has existed for just under 40 years. In essence, a secure multiparty computation protocol is executed by two or more parties who wish to jointly compute the output of an arbitrary function, without sacrificing the privacy of their respective inputs. Initially, MPC was branded as a purely theoretical concept, however since the late 2000s, it has been used to solve a myriad of real-world problems. As the adoption of MPC continues to increases within everyday applications, it is now essential for information security practitioners to be aware of the fundamental concepts underpinning its functionality.

In the first half of this report, we aim to provide a thorough overview of secure multiparty computation, ranging from the mathematical primitives that are commonly used to construct MPC protocols, to the current and future applications of MPC as a whole. With a view to appeal to an audience with a wide range of mathematical abilities, we have included detailed examples and explanations throughout.

In the second half of this report, we apply our newly attained knowledge to a particular application of MPC, namely threshold signature schemes, and their potential application within digital asset self-custody solutions. Our main focus in relation to this is a state-of-the-art threshold Schnorr signature scheme known as FROST, which we deconstruct with the aim of not only providing a detailed summary of its operation, but further how its goals are achieved through the use of secure multiparty computation. FROST is a relatively new threshold signature scheme, having only been introduced by Komlo et al. in December 2020. As such, it is yet to be implemented and utilised for any real-world applications. Therefore, as a part of this report we have also produced a proof-of-concept Python implementation and demonstration of FROST. Finally, we compare FROST to three other mechanisms, including a multi-signature scheme known as MuSig2, with a view to consider the benefits and drawbacks of utilising each in the context of digital asset self-custody.