On efficient tee-assisted verifiable secret sharing for confidential storage

Context and objectives

This research work focuses on enhancing the performance of verifiable secret sharing protocols. These protocols are particularly used for confidential storage. A typical scenario is that of a user who wants to have their files hosted on a cloud, or a multicloud, but does not want the host to have access to the contents of their files. In this case, the user will encrypt their files and store both the encrypted files and the used encryption keys on the cloud. Verifiable secret sharing protocols are used when uploading encryption keys. These protocols consists of methods to split and distribut a secret, in this case keys, within a group of nodes in such a way that no single node has sufficient information to recover the original secret, but when a sufficient number of nodes combine their secret share, the latter can then be reconstituted. The verifiable nature of these protocols ensures that even if the node (or if the user) initiating the secret sharing is malicious/corrupted, it will still be possible to reconstruct the secret.

These protocols operate in two steps, a secret sharing phase, and a secret reconstruction phase. Each phase requires several "rounds" of communication between the participating nodes to ensure correct execution, despite the presence of a certain number f of malicious nodes that will attempt to prevent both phases from completing, and will also try to retrieve the shared secret. In doing so, these protocols impose a high cost in their use, due to the high message complexity and the cryptographic tools required.

The aim of this research work is to revisit verifiable secret sharing protocols in order to improve their performance thanks to Trusted Execution Environments (TEEs such as Intel SGX) that guarantees the integrity of the code executed by the nodes, thus transforming any potentially malicious node behavior into crash faults in the worst case, and making it possible to reduce message complexity and the cryptographic tools used.

Methodology:

#1 - The first step of this work is to review existing approaches to verifiable secret sharing, including publicly verifiable secret sharing.

#2 - The second step will be to transform a subset of the identified protocols into less costly protocols using only or partially nodes benefiting from the properties of trusted execution technologies such as Intel SGX.

#3 - The third step of this work will consist of evaluating the proposed approaches in order to experimentally quantify the impact of the various proposed approaches compared with solutions that do not use TEEs.

Supervisors (LaBRI – University of Bordeaux) :
Joachim Bruneau-Queyreix – joachim.bruneau-queyreix@u-bordeaux.fr
Laurent Réveillère – laurent.reveillere@u-bordeaux.fr