THRESHOLD SIGNATURES WITH OFFLINE PARTIES

Alessio Meneghetti

Università degli Studi di Trento

Digital Signatures are widely used in blockchain-based platforms. For instance, such decentralised applications make use of them to guarantee property of digital assets: only one in possession of the right private key is the owner of the corresponding asset. This idea cannot however be safely applied to situations in which more parties share the ownership of the asset, at least when using the most common digital signatures schemes such as RSA or ECDSA. A possible solution lies in (t,n)-threshold signature schemes, protocols enabling distributed signing among n players, with the rule that at least t among them have to agree on the signature. Most of the schemes produce signatures that are compatible with existing centralized signature schemes. In this context, the key-generation and signature algorithms are replaced by a communication protocol between the parties, while the verification algorithm remains identical to that of a signature issued using the centralized algorithm. A limitation of these schemes is that all involved parties need to be active during the key-generation phase. After a brief introduction to classical and threshold Digital Signatures, I will present a recent (2,3)-threshold signature with a key-generation phase allowing the absence of one among the three parties.