ORCAS - An Efficient Adaptor Signature based on CSI-FiSh

Silvia Sconza

Abstract: An adaptor signature is a variant of a digital signature that embeds a secret into the signing process, generating a pre-signature. The resulting pre-signature can be turned into a valid signature only by someone who knows that secret, and in doing so, the secret becomes publicly extractable. A typical use case is the atomic swap, which allows two parties who do not trust each other to safely exchange digital assets without relying on a trusted third party.

We present One-Round "Cheating" Adaptor Signatures (ORCAS), a novel and efficient construction based on CSI-FiSh. Our protocol offers significant improvements over previous proposals: unlike IAS (Tairi et al., FC 2021), it avoids costly non-interactive zero-knowledge proofs, and unlike adaptor MCSI-FiSh (Jana et al., CANS 2024), it does not require modifying the underlying digital signature scheme.