

In cryptography, adaptor signatures extend standard digital signatures. They allow the signer to make a promise on an actual signature, which is then revealed in exchange for a secret value. This functionality of adaptor signatures has recently been used in many applications regarding cryptocurrencies, including conditional payments. This thesis studies the security of adaptor signatures for Schnorr signature and ECDSA motivated by the conditional payments. We identify limitations of existing security definitions when applied to practical adaptor signatures for ECDSA and provide an example of such a limitation in the context of the Bitcoin blockchain. To address these problems, we present new security definitions and prove that the practical adaptor signature for ECDSA satisfies our notion of security.