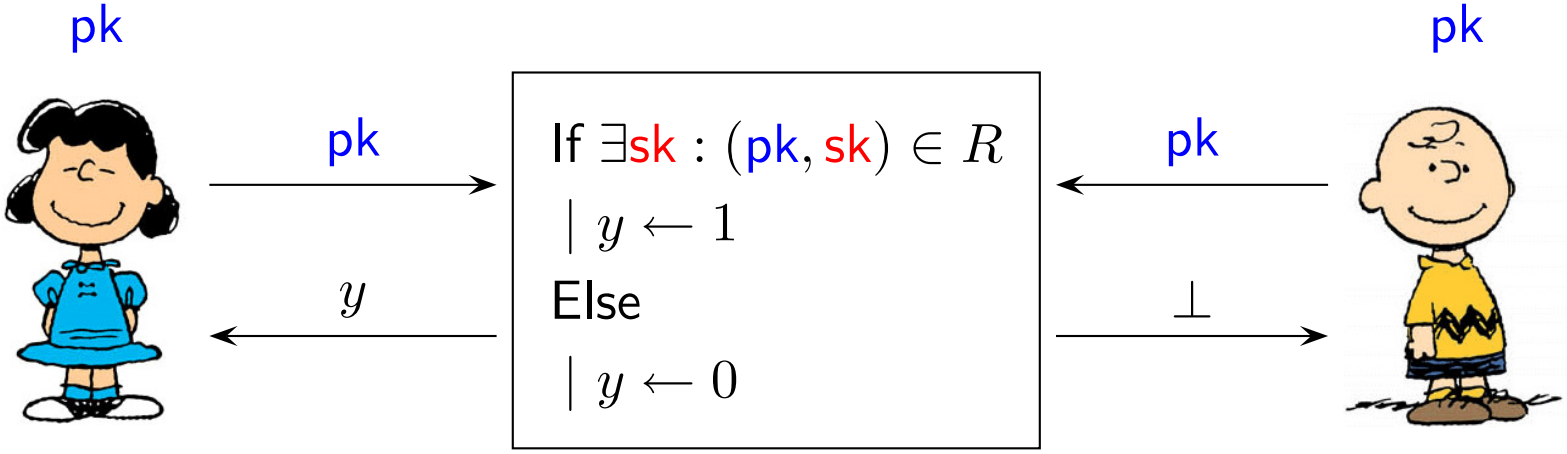
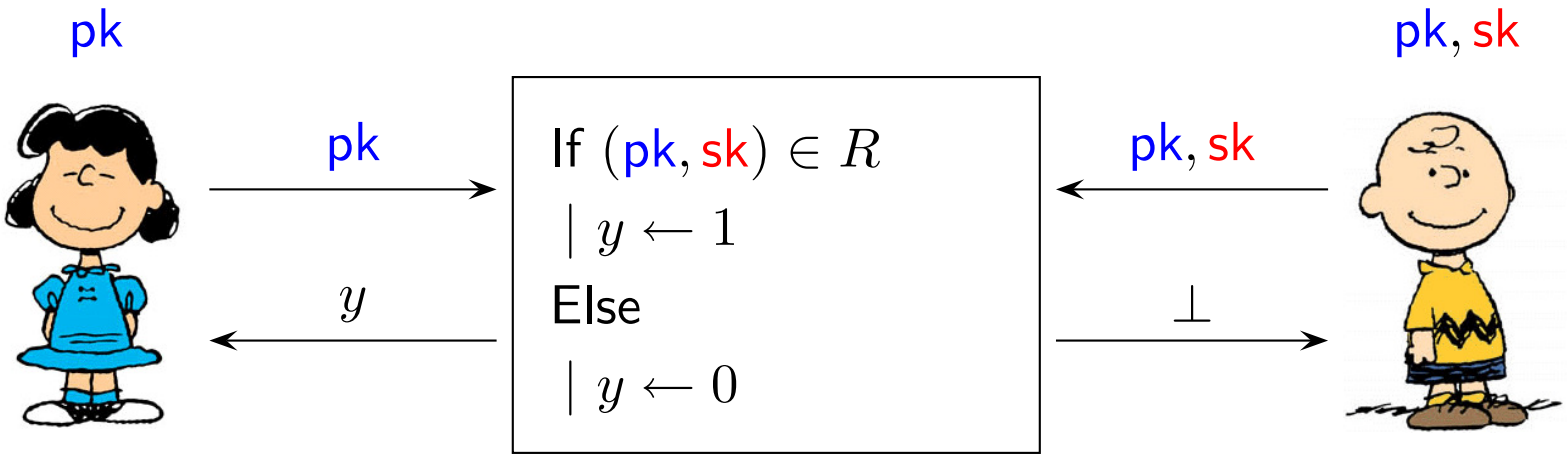
An ideal implementation of a zero-knowledge proof



An ideal implementation of a zero-knowledge proof of knowledge