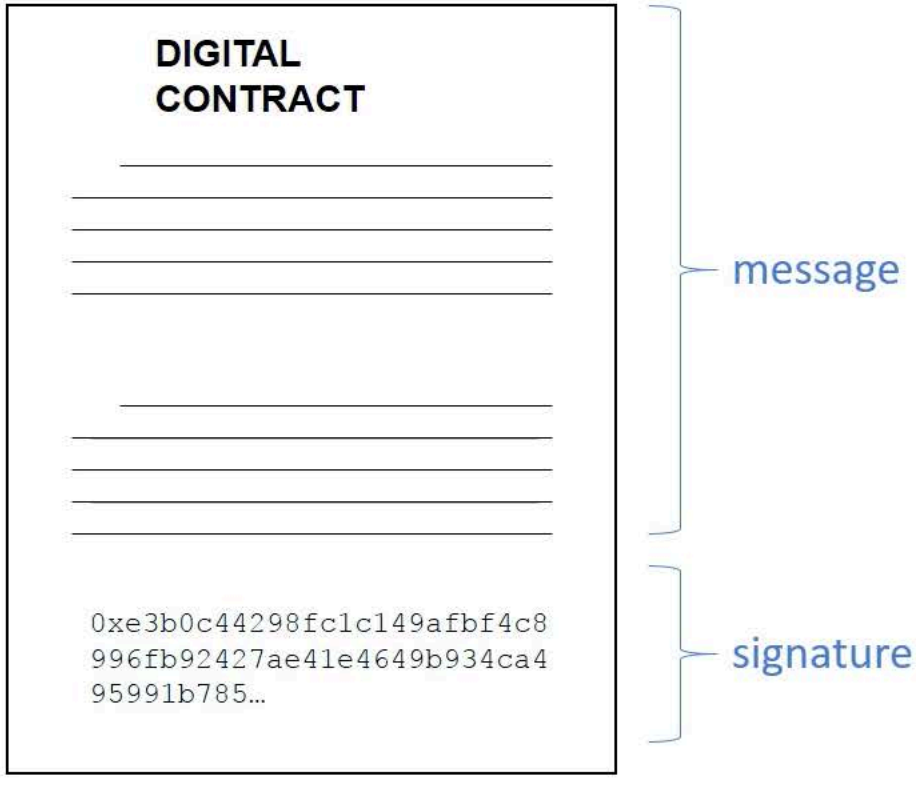
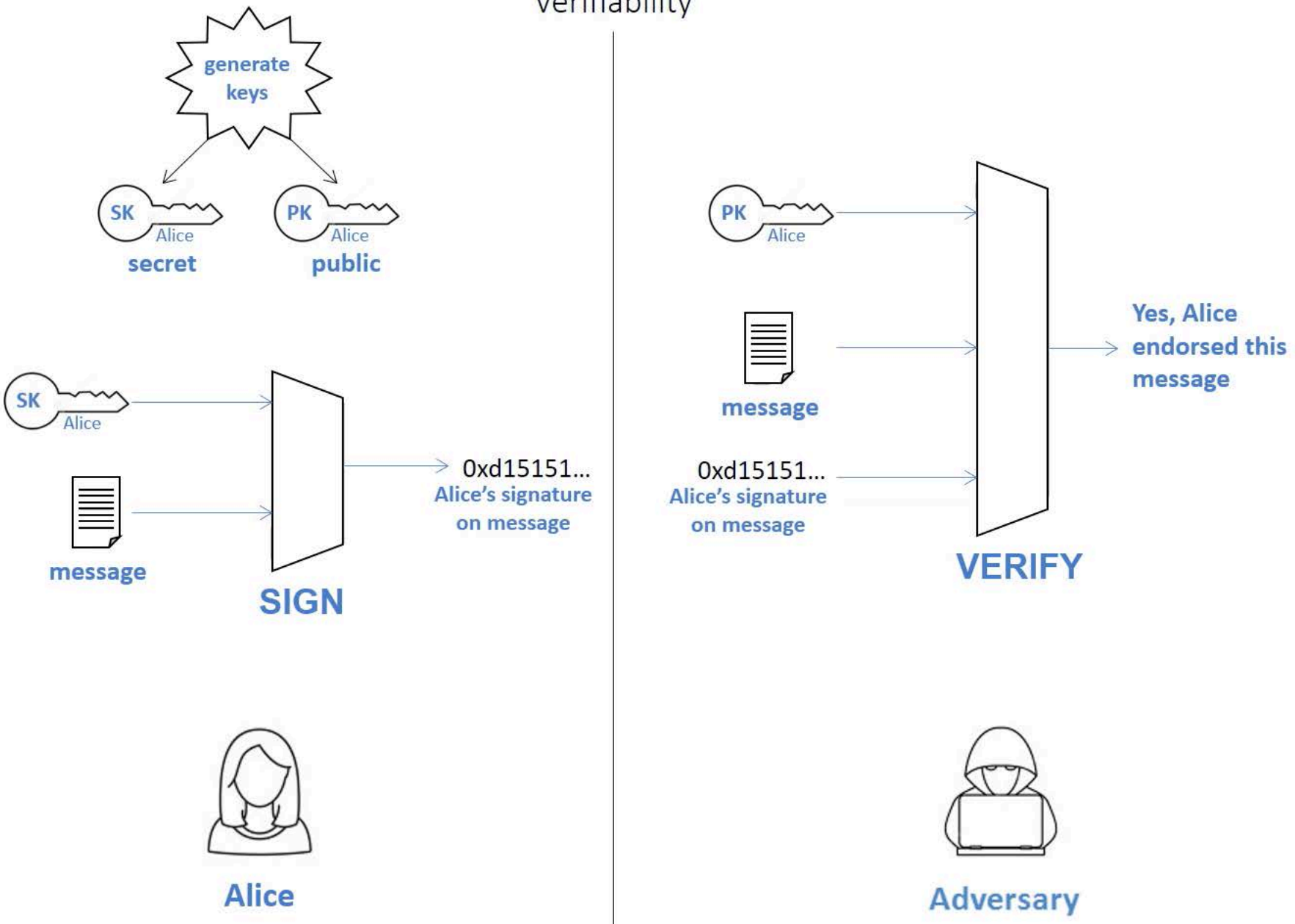
Digital Signatures

1. Verifiability: Only Alice can make her signature, but anyone who sees it can verify that it's valid.
2. Unforgeability: The signature is tied to a particular message, so that the signature cannot be used to indicate Alice's endorsement of a different message.

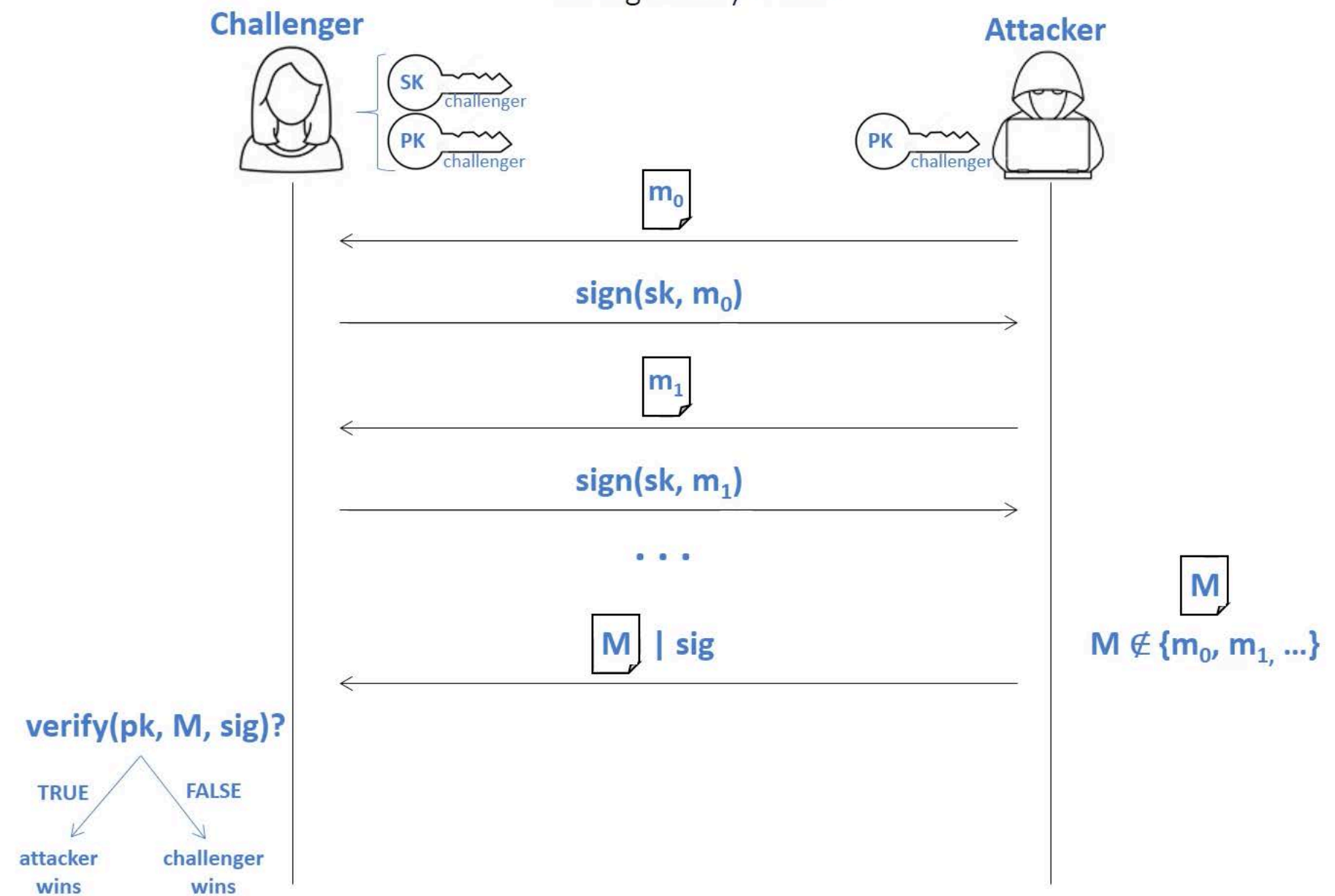


Digital Signatures
Verifiability



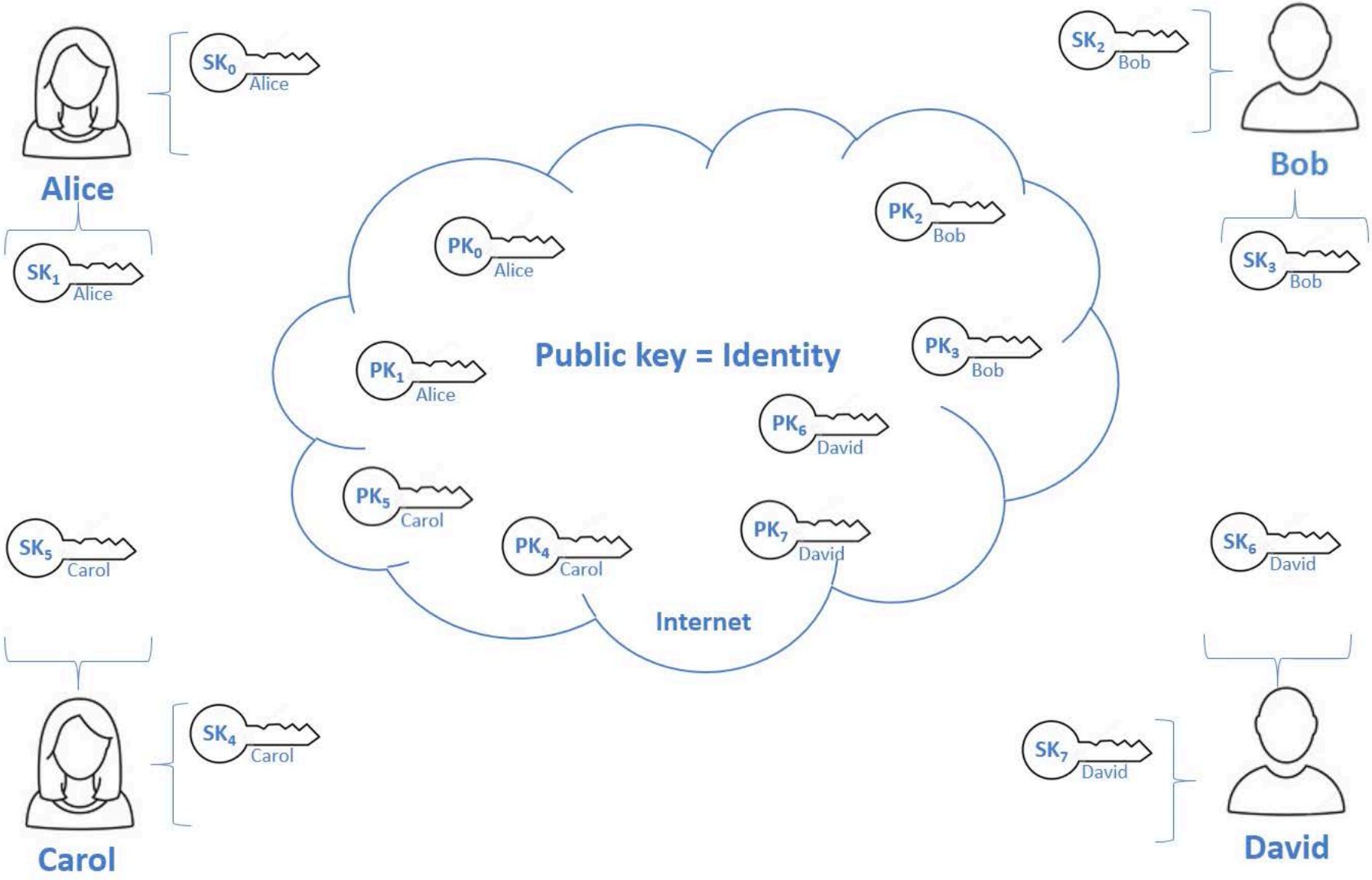
Digital Signatures

Unforgeability Game



Decentralized Identity Management

Public Keys as Identities



A person can generate multiple public keys, and thus can have multiple identities