
Claims, Credentials, Anonymity and Privacy Technologies
1. Digital Identity and Credentials
Verifiable Digital Identities
Decentralized Identifiers (DIDs)
Digital Certificates
Tokenized Identity
Distributed Identity
Credentials
Verifiable Credentials (VCs)
Attribute-Based Credentials
Blind Credentials
Selective Disclosure
Infrastructure
Public Key Infrastructure (PKI)
2. Cryptographic Signature Schemes
Individual and Anonymous Signatures
Digital Signature
One-Time Signatures
Homomorphic Signatures
Blind Signatures
Threshold Signatures
Group and Anonymous Schemes
Group Signature
Ring Signature
Linkable Ring Signatures
Ephemeral Keys
3. Privacy and Anonymity Techniques
Anonymity and Unlinkability
Pseudonymity
Stealth Addresses
Mix Networks (Mixnets)
Monerozeroth
Privacy-Enhancing Transactions
Confidential Transactions
Confidentiality
Salt
4. Zero-Knowledge and Privacy Proofs
Zero-Knowledge Proof Technologies
Zero-Knowledge Proofs (ZKP)
Non-Interactive Zero-Knowledge Proofs (NIZK)
zk-SNARKs
zk-STARKs
Bulletproofs
BOLT
Advanced Applications
Selective Disclosure
Secure Multi-Party Computation (SMPC)
5. Cryptographic Primitives & Functions
Hash and Random Functions
Cryptographic Hash Functions
Chameleon Hashes
Verifiable Random Functions (VRF)
Pseudorandom Functions (PRF)
Oblivious Pseudorandom Functions (OPRF)
Encryption & Key Management
Identity-Based Encryption (IBE)
PGP (Pretty Good Privacy)
Secure Enclaves / Trusted Execution Environments (TEE)
6. Privacy & Security Ecosystem
Standards and Frameworks
Privacy-Enhancing Technologies (PETs)
Digital Certificates
Protocols and Implementations
Verifiable Credentials: Enable users to share only necessary personal information selectively.
Ring Signatures: Facilitate anonymous cryptocurrency transactions.
Secure Multi-Party Computation: Collaborative data analysis without exposing private data.
Zero-Knowledge Proofs: Prove statements (e.g., age, creditworthiness) without revealing sensitive details.