

Digital Identity, Privacy, and Cryptographic Technologies Mind Map

Digital Identity & Credentials

- CREdentialia & Identity
 - Credentials
 - Identity claims
 - Authenticity
- Claims
 - Ownership
 - Attributes
 - Verification

Cryptographic Infrastructure

- Public Key Infrastructure (PKI)
 - Public key
 - Private key
 - PGP
- Private Key Infrastructure
 - Key management
 - Secure storage

Privacy & Anonymity Tools

- Identity Mixers
 - Anonymity enhancement
 - Mixture and mixing protocols
- Anonymity Mechanisms
 - Network layer privacy (TOR, VPN)
 - Salt
 - Confidentiality

Digital Signatures & Advanced Cryptography

- Standard & Blind Signatures
 - Digital signature
 - Blind signature
- Group & Ring-based Schemes
 - Group signature
 - Ring signature
 - Ringet
- Zero-Knowledge Proofs
 - Zero knowledge SNARK
 - Zero knowledge STARK
 - Zero knowledge rollups
 - Bulletproof
 - BOLT

Privacy-Preserving Transactions & Coins

- Coin Mixing & Obfuscation
 - CoinJoin
 - CoinSwap / Shuffle
- Privacy Coins
 - Monero
 - Zcash

Cryptographic Primitives

- PRF and Extensions
 - PRF (Pseudorandom Function)
 - HMAC-KDF
 - OPRF (Oblivious PRF)
- Homomorphic Encryption
 - Secure digital identity verification
 - Privacy-preserving financial transactions
 - Confidential communication and messaging
 - SHE (Somewhat HE)