Kryptografia

Rafał Włodarczyk

INA 6, 2026

1. BLS Signature
2. RSA
3. Diffie-Hellman KEX
4. Fiat-Shamir Transform
5. Sigma Protocol

1. Noninteractive Identification Scheme (Schnorr)
2. Signature Scheme (Schnorr, Ring Signature)
3. Interactive Schemes (BLS Signature)
4. AKE - Authenticated Key Exchange ,- Both parties calculate (1) the same key, (2) the key is secret, (3) both parties prove their identity
5. Encryption Ciphersystems (El Gamal), Basic El Gamal is reciphering prone - no CCA2 compliance.
6. Reciphering - Randomized Partial Checking. - Voting Credibility Problem
7. Secure Multiparty Computation (Problem Bizantyjskich Generałów - Byzantine Agreement)
8. Schematy Progowe - Shamir Secret Sharing
9. Prime Decomposition Problem, Discrete Logarithm Problem, Computation, Decisional - Diffie-Hellman Problem
10. Oblivious Transfer (OT)
11. Private Set Intersection (PSI)
12. Private Set Intersection Caridinality (PSI-CA)
13. Signcryption - Signing and Encryption at Once.

Models:

1. Signature Oracle

2. Encryption Oracle
3. Decryption Oracle
4. Random Oracle - Perfect Hashing Function
5. CCA, CCA2 - Decryption Oracle after receiving a Challenge. Reszyfracja