



[1] Dolev, Yao. On the Security of Public Key Protocols. 1963
[2] Blanchet. Modeling and Verifying Security Protocols with the applied Pi Calculus and ProVerif. 2016
[3] Blanchet. An Efficient Cryptographic Verifier Based on Prolog Rules. 2001
[4] Ballare, Rogaway. Random Oracles are Practical: A Paradigm for Designing Efficient Protocols. 1995
[5] Abadi, Rogaway. Reconciling Two Views of Cryptography. 2002
[6] Shoup. Sequences of Games: a Tool for Taming Complexity in Security Proofs. 2004
[7] Blanchet. A Computationally Sound Mechanized Prover for Security Protocols. 2006
[8] Blanchet, Pointcheval. Automated Security Proofs with Sequences of Games. Advances in Cryptology. 2006