

[8] Blanchet, Pointcheval. Automated Security Proofs with Sequences of Games. Advances in Cryptology. 2006