Security Protocols and Verification

Design and Analysis of Cryptographic Protocols

Garance Frolla
Ely Marthouret
Ewan Decima

September / November 2025

1 Assumptions

We assume that at the beginning of the protocol agents A and B know the public key $K_{pub(C)}$ of any agent C. Moreover, we assume that all agents C shared a symmetric key with a trusted server S, named K_{CS}. N_a is a nonce generated by A, and N_b is a nonce generated by B. τ and λ respectively denote a timestamp and a lifetime. A generates K_{AB} with perfect randomness at each session. .

2 Protocol: Ely the frog

1. $A \to B : \{|A, B, Secret|\}_{pub(B)}$
2. $A \to S : \{|A, B, T_A, K_{AB}|\}_{K_{AS}}$
3. $S \to B : \{|A, B, T_S, K_{AB}|\}_{K_{BS}}$
4. $A \to B : \{|A, B, message, Secret|\}_{K_{AB}}$