Security Protocols and Verification

Design and Analysis of Cryptographic Protocols

Garance Frolla
Ely Marthouret
Ewan Decima

September / November 2025

1 Protocol: Ely the frog

1. $A \to B : \{A, B, N_A\}_{pub(B)}$
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. $B \to A : \{|B, A, N_A + 1|\}_{K_{AB}}$