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: First Attempt

1. $A \to S : \{|A, B, N_a, K_{AB}|\}_{K_{AS}}$
2. $S \to A : \left\{ \left| S, A, N_a + 1, \{|A, B, K_{AB}, N_a, \tau, \lambda|\}_{K_{BS}} \right| \right\}_{K_{AS}}$
3. $A \to B : \{|A, B, K_{AB}, N_a, \tau, \lambda, |\}_{K_{BS}}$
4. $B \to S : \{|B, A, N_b|\}_{K_{BS}}$
5. $S \to B : \{|S, B, N_b + 1, h(K_{AB}, N_b)|\}_{K_{BS}}$
6. $B \to A : \{B, A, N_a + 1, h(K_{AB}, N_b)\}_{pub(A)}$
7. $A \to B : \{A, B, N_b + 1, h(K_{AB}, N_a)\}_{pub(B)}$

3 Fourth Attempt

1. $A \rightarrow S : \{|A, B, N_a, K_{AB}|\}_{K_{AS}}$
2. $S \rightarrow A : \left\{ \left| A, N_a + 1, \{|A, B, N_a, \tau, \lambda, K_{AB}|\}_{K_{BS}} \right| \right\}_{K_{AS}}$
3. $A \rightarrow B : \{|A, B, N_a, \tau, \lambda, K_{AB}|\}_{K_{BS}}$
4. $B \rightarrow A : \{B, A, N_a + 1, h(K_{AB}, N_a)\}_{pub(A)}$

4 Protocol: Pub and Priv

1. $A \rightarrow B : \left\{ \{A, N_A, K_{AB}\}_{priv(A)} \right\}_{pub(B)}$
2. $B \rightarrow A : \left\{ \{B, N_A + 1, h(K_{AB})\}_{priv(B)} \right\}_{pub(A)}$

This *perfect* protocol does not conform to the requirement equations.

5 Protocol: pub + Kab

1. $A \rightarrow B : \left\{ \{A, N_A, K_{AB}\}_{pub(B)} \right.$
2. $B \rightarrow A : \left\{ \{B, N_A, N_B\}_{pub(A)} \right.$
3. $A \rightarrow B : \left\{ \{A, N_B\}_{Kab} \right.$
4. $B \rightarrow A : \left\{ \{B, N_A\}_{Kab} \right.$

6 Protocol: pub only

1. $A \rightarrow B : \left\{ \{A, N_A, K_{AB}\}_{pub(B)} \right.$
2. $B \rightarrow A : \left\{ \{N_A, N_B\}_{pub(A)} \right.$
3. $A \rightarrow B : \left\{ \{N_B\}_{pub(B)} \right.$
4. $B \rightarrow A : \left\{ \{h(Kab)\}_{pub(A)} \right.$

7 Protocol: Ely the frog

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

We can reduce the cost on the last message using the hash function :

1. $A \rightarrow B : \{A, B, N_A\}_{pub(B)}$
2. $A \rightarrow S : \{|A, B, T_A, K_{AB}|\}_{K_{AS}}$
3. $S \rightarrow B : \{|A, B, T_S, K_{AB}|\}_{K_{BS}}$
4. $B \rightarrow A : \{B, N_A + 1, h(K_{AB})\}_{pub(A)}$

8 Ely the big frog

1. $A \rightarrow B : \{A, \{|N_A|\}_{K_{AB}}\}_{pub(B)}$
2. $A \rightarrow S : \{B, \tau, \lambda, K_{AB}\}_{K_{AS}}$
3. $S \rightarrow B : \{A, \tau, \lambda, K_{AB}\}_{K_{BS}}$
4. $A \rightarrow B : \{B, N_A + 1\}_{pub(A)}$