L'équipe Proto-Chorale attaque le protocole NSAv2

Cardinaël Loïc, Klein Elise, Bidault Clément

October 2020

1 Objectif

L'objectif de cette attaque pour C est d'envoyer K_{bc} au nom de A.

2 Scénario de l'attaque

On suppose que A entame des discussions avec B et C :

1. $A \rightarrow S : A, \{B\}_{Kas}$
2. $A \rightarrow S : A, \{C\}_{Kas}$
3. $S \rightarrow B : S, \{A, N_1\}_{K_{bs}}$
4. $S \rightarrow C : S, \{A, N_2\}_{K_{cs}}$
5. $S \rightarrow A : S, \{N_1\}_{K_{as}}$: **inversion d'entête avec (6)**, ce message passe pour venant de **C**
6. $S \rightarrow A : S, \{N_2\}_{K_{as}}$: **inversion d'entête avec (5)**, ce message passe pour venant de **B**
7. $A \rightarrow C : \{N_1, K_{ac}\}_{pub(C)}$ **C apprend** N_1
8. $A \rightarrow B : \{N_2, K_{ab}\}_{pub(B)}$ **C bloque le message**
9. $C \rightarrow B : \{N_1, K_{bc}\}_{pub(B)}$ **B reçoit** K_{bc}**, convaincu qu'elle vient de A**
10. $B \rightarrow A : \{K_{bc}\}_{pub(A)}$ **C bloque ce message.** B termine sans se rendre compte du problème.