L'équipe Proto-Chorale attaque le protocole AzoteV2

Cardinaël Loïc, Klein Elise, Bidault Clément

October 2020

1 Objectif

L'objectif de l'attaque est de faire terminer le processus à A sans que B n'ait reçu la clé.

2 Scénario de l'attaque

Le protocole se déroule normalement entre A et B jusqu'à ce que C bloque $S \rightarrow B : \{K_{ab}\}_{K_{bs}}$. Le protocole se termine avec A qui pense que tout s'est bien passé, alors que B n'a pas reçu la clé. B a certes aperçu le problème avec le dernier message, mais n'a aucun moyen d'en prévenir A.
Ainsi, la propriété "Si A a fini en ayant envoyé une clé K à B, alors B a bien reçu K de la part de A." n'est pas vérifiée.