L'équipe Proto-Chorale attaque le protocole TAZv3

Cardinaël Loïc, Klein Elise, Bidault Clément

October 2020

1 Objectif

L'objectif de cette attaque pour C est d'envoyer à B le nonce N_a en se faisant passer pour A.

2 Scénario de l'attaque

A initie une communication avec C, que ce dernier va utiliser pour discuter avec B :

- $A \rightarrow C : \{Na\}_{pub(C)}$
- $C(A) \rightarrow B : \{Na\}_{pub(B)}$
- $B \rightarrow A : \{\{N_b\}_{N_a}\}_{pub(A)}, h(N_a)$
- $A \rightarrow C \rightarrow B : h(N_b)$ A et B terminent normalement

3 Conclusion

La propriété d'authentification n'est pas respectée.