L'équipe Proto-Chorale attaque le protocole QG V3

Cardinaël Loïc, Klein Elise, Bidault Clément

October 2020

1 Objectif

L'objectif est de déchiffrer scrt et de se faire passer pour B aux yeux de A.

2 Scénario de l'attaque

A entame un conversation normale avec B, suivi de C qui va recopier le premier nonce :

1. $A \rightarrow B : A, \{N_a\}_{pub(B)}$
2. $C \rightarrow B : C, \{N_a\}_{pub(B)}$
3. $B \rightarrow A : \{N_a\}_{pub(A)}, \{B, N_b\}_{pub(A)}$, message bloqué par C.
4. $B \rightarrow C : \{N_a\}_{pub(C)}, \{B, N'_b\}_{pub(C)}$
5. $C(B) \rightarrow A : \{N_a\}_{pub(A)}, \{B, N'_b\}_{pub(A)}$
6. $A \rightarrow B : \{\{scrt\}_{N'_b}\}_{N_a}$, message bloqué par C, qui récupère le secret car connaissant les deux nonces
7. $C(B) \rightarrow A : \{scrt\}_{pub(A)}$, A termine en pensant que B a bien reçu la clé, mais c'est C qui l'a récupéré.

3 Conclusion

Les propriétés de confidentialité, et d'authentification de B ne sont pas respectées