L'équipe Proto-Chorale attaque le protocole QGv2

Cardinaël Loïc, Klein Elise, Bidault Clément

October 2020

1 Objectif

L'objectif de cette attaque pour C est de connaître scrt.

2 Scénario de l'attaque

- $A \to B : A, \{N_a\}_{pub(B)}$
- $B \to A : \{N_a\}_{pub(A)}, \{N_{ba}\}_{pub(A)}$, ce message est **bloqué** par C.

C récupère de quoi entamer sa discussion avec B :

- $C \to B : C, \{N_a\}_{pub(B)}$
- $B \to C : \{N_a\}_{pub(C)}, \{N_{bc}\}_{pub(C)}$, **C connaît** N_a **et** N_{bc}**.**
- $C(B) \to A : \{N_a\}_{pub(A)}, \{N_{bc}\}_{pub(A)}$

A va alors envoyer le secret, lisible par C, et C va s'assurer que sa discussion avec B se termine correctement :

- $A \to B : \{scrt\}_{\{N_{bc}\}_{N_a}}$ C peut lire le secret. **Il bloque ce message.**
- $C \to B : \{scrt\}_{\{N_{bc}\}_{N_a}}$
- $B \to C : \{scrt\}_{pub(C)}$ B finit sa communication avec C, satisfait.

C va maintenant s'assurer que A et B terminent bien leur conversation :

- $C \to A : C, \{N_{ba}\}_{pub(A)}$
- $A \to C : \{N_{ba}\}_{pub(C)}, \{N_{ac}\}_{pub(C)}$
- $C \to B : \{scrt\}_{\{N_{ba}\}_{N_a}}$ on peut même remplacer scrt à ce stade pour casser l'authenticité.
- $B \to A : \{scrt\}_{pub(A)}$, A et B pensent avoir fini normalement leur conversation.

3 Conclusion

La propriété de confidentialité est cassée.