# L'équipe Proto-Chorale attaque le protocole QG

Cardinaël Loïc, Klein Elise, Bidault Clément

October 2020

## 1 Objectif

L'objectif de l'attaque est de déchiffrer scrt, en reposant sur la confusion de type entre un agent et une nonce.

## 2 Scénario de l'attaque

1. $A \rightarrow B : A, \{N_a\}_{pub(B)}$ Etape normale
2. $B \rightarrow A : SYM\{B\}_{N_a}, \{N_b\}_{pub(A)}$ Ce message sera bloqué par C
3. $C(B) \rightarrow A : SYM\{B\}_{N_a}, \{B\}_{pub(A)}$ C veut utiliser comme deuxième nonce B au lieu de $N_b$ en se faisant passer pour B
4. $A \rightarrow B : A, \{scrt\}_{SYM\{B\}_{N_a}}$ C a vu passer $SYM\{B\}_{N_a}$ sur le message bloqué, et peut donc déchiffrer scrt et le lire. C bloque ce message.
5. $C(B) \rightarrow A : h(scrt)$ A a fini sa session.

## 3 Conclusion

La propriété de confidentialité n'est pas respectée au regard de cette attaque.