Attaque sur le protocole QG

Johan Tombre, Vivien Maintenant, Paul Gellenoncourt

Description de l'attaque :
Lorsque C va recevoir le premier message de A, il va déchiffrer N_a pour le chiffrer avec la clé publique de B puis envoyer le message A, $\{N_a\}_{pub(B)}$ à B. Cela marque le début d'un échange entre A et B initié par C. B va alors générer un nonce N_b pour le transmettre à A. En recevant ce message, A pense qu'il provient de C et va donc chiffrer son secret avec la combinaison des nonce N_a et N_b à C. C transmet simplement ce message à B qui va pouvoir le déchiffrer et transmettre ce même secret chiffré avec la clé publique de A.

$$A \rightarrow C : A, \{N_a\}_{pub(C)}$$
$$C(A) \rightarrow B : A, \{N_a\}_{pub(B)}$$
$$B \rightarrow A : \{N_a\}_{pub(A)}, \{N_b\}_{pub(A)}$$
$$A \rightarrow C : \{scrt\}_{SYM\{Na\}Nb}$$
$$C(A) \rightarrow B : \{scrt\}_{SYM\{Na\}Nb}$$
$$B \rightarrow A : \{scrt\}_{pub(A)}$$

Conclusion : Lorsque le protocole finit, A pense avoir réalisé un échange avec C alors qu'il a communiqué avec B. B, quant à lui, pense avoir réalisé un échange normal avec A.