Attaque du protocole REX

Clément Bidault, Loïc Cardinaël, Elise Klein

On peut effectuer une attaque "*Man-in-the-middle*" sur le protocole de la manière suivante :

$$
\begin{array}{l}
A \rightarrow C : \{A, K_{ab}\}_{pub(C)} \\
C \rightarrow B : \{A, K_{ab}\}_{pub(B)} \\
B \rightarrow C(A) : B, \{h(K_{ab}), N_b\}_{pub(A)} \\
C \rightarrow A : C, \{h(K_{ab}), N_b\}_{pub(A)} \\
A \rightarrow C : \{N_b, K\}_{K_{ab}} \\
C \rightarrow B : \{N_b, K'\}_{K_{ab}}
\end{array}
$$

La troisième ligne signifie que C intercepte le message de B pour A et le modifie avant de le renvoyer à A.

A la fin de l'attaque, B pense avoir échangé avec A et pense que K' est le secret envoyé par A. La propriété "Si B a fini pensant avoir recu une clef K venant de A, alors A a bien envoyé K à B." n'est donc pas vérifiée.