Needham-Schroeder 認證協定

- 1978 年兩人提出『多重盤問與回應』協定
  - 利用 N_1、N_2、N_3 ， N_1預防重複連線
  - 連線識別(類似 TCP 三向式握手式連絡法)
- 通行票：Ticket = $E_{KB}[ID_A \| K_S]$
- 可能遭受重播攻擊 (訊號 (3))