

Synthesized solution for benchmark `01asendrecv.c`

solution

The diagram illustrates a formal proof tree for the security of the Needham-Schroeder protocol. The root node is labeled $(\text{Partial}), \text{cond } b_{11}: b > 0$. The proof proceeds through several nested cases and conditions:

- Case b_{11} :**
 - Sub-cases k_1 and k_2 define initial protocol states and messages.
 - Condition $(\text{Partial}), \text{cond } b_{26}: b > 0$ leads to **Case b_{26} :**
 - Sub-cases k_1 and k_2 define intermediate states.
 - Condition $(\text{Partial}), \text{cond } c_{23}: \text{auth} > 0$ leads to **Case c_{23} :**
 - Sub-cases k_1 and k_2 define states involving M_{auth} .
 - AComplete** node leads to **Axioms** ($\{I = 1, J = 1, M = 1, P = 1\}$).
- Case $\neg b_{11}$:**
 - Sub-cases k_1 and k_2 define alternative initial states.
 - Condition $(\text{Partial}), \text{cond } c_{23}: \text{auth} > 0$ leads to **Case c_{23} :**
 - Sub-cases k_1 and k_2 define states involving J_{auth} .
 - Condition $(\text{Partial}), \text{cond } b_{26}: b > 0$ leads to **Case $\neg b_{26}$:**
 - Sub-cases k_1 and k_2 define states involving J_{auth} and I_{cond} .
 - AComplete** node leads to **Axioms** ($\{I = 1, J = 1\}$).

The proof concludes with **AComplete** nodes and **Axioms** sets, demonstrating the validity of the protocol's security properties under the given conditions.

Remaining 37 solutions omitted for brevity.