MODULE $BBB4P$

EXTENDS $Naturals$, $Sequences$

CONSTANT $QuantumStates$, $CurrentTimestamp$

VARIABLES $aliceState$, $bobState$, $channelState$, $qubitState$,
$qubitLocation$, $eveInterfered$, $transferred$, $auditTrail$

$Init \triangleq$
$\land\ aliceState = \text{“hasQubit”}$
$\land\ bobState = \text{“waiting”}$
$\land\ channelState = \text{“ready”}$
$\land\ qubitState \in QuantumStates$
$\land\ qubitLocation = \text{“alice”}$
$\land\ eveInterfered = \text{FALSE}$
$\land\ transferred = \text{FALSE}$
$\land\ auditTrail = \langle\rangle$

$PrepareEntanglement \triangleq$
$\land\ aliceState = \text{“hasQubit”} \land channelState = \text{“ready”}$
$\land\ channelState' = \text{“entangled”}$
$\land\ \text{UNCHANGED}\ \langle aliceState, bobState, qubitState, qubitLocation, transferred, eveInterfered, auditTrail\rangle$

$TeleportQubit \triangleq$
$\land\ channelState = \text{“entangled”} \land aliceState = \text{“hasQubit”}$
$\land\ aliceState' = \text{“sent”}$
$\land\ channelState' = \text{“used”}$
$\land\ qubitLocation' = \text{“inChannel”}$
$\land\ transferred' = \text{TRUE}$
$\land\ \text{UNCHANGED}\ \langle bobState, qubitState, eveInterfered, auditTrail\rangle$

$ReceiveAtBob \triangleq$
$\land\ transferred = \text{TRUE} \land qubitLocation = \text{“inChannel”} \land bobState = \text{“waiting”}$
$\land\ bobState' = \text{“received”}$
$\land\ qubitLocation' = \text{“bob”}$
$\land\ auditTrail' = Append(auditTrail, [type \mapsto \text{“BB4P-transfer”}, time \mapsto CurrentTimestamp])$
$\land\ \text{UNCHANGED}\ \langle aliceState, qubitState, channelState, eveInterfered, transferred\rangle$

$Eavesdrop \triangleq$
$\land\ qubitLocation = \text{“inChannel”} \land eveInterfered = \text{FALSE}$
$\land\ eveInterfered' = \text{TRUE}$
$\land\ qubitLocation' = \text{“eavesdropper”}$
$\land\ qubitState' = \text{“collapsed”}$ Qubit is destroyed
$\land\ channelState' = \text{“tampered”}$
$\land\ \text{UNCHANGED}\ \langle aliceState, bobState, auditTrail, transferred\rangle$

$Next \triangleq PrepareEntanglement \lor TeleportQubit \lor ReceiveAtBob \lor Eavesdrop$

$Spec \triangleq Init \land \Box[Next]_{\langle aliceState,\ bobState,\ channelState,\ qubitState,\ qubitLocation,\ eveInterfered,\ transferred,\ auditTrail\rangle}$

$NoCloning \triangleq qubitLocation \in \{\text{“alice”}, \text{“bob”}, \text{“inChannel”}, \text{“eavesdropper”}, \text{“lost”}\}$

$NoUndetectableEavesdropping \triangleq eveInterfered = \text{TRUE} \Rightarrow qubitState = \text{“collapsed”}$

$$\begin{aligned} Correctness \triangleq\ & bobState = \text{“received”} \\ \Rightarrow\ & \land\ qubitState \neq \text{“collapsed”} \\ & \land\ qubitLocation = \text{“bob”} \\ & \land\ channelState = \text{“used”} \end{aligned}$$

$BB4PTransfers(trail) \triangleq \{t \in trail : t.type = \text{“BB4P-transfer”}\}$

$ExactlyOneAudit \triangleq Len(BB4PTransfers(auditTrail)) = 1$

$$\begin{aligned} &INVARIANTS \triangleq \\ &\quad \land\ NoCloning \\ &\quad \land\ NoUndetectableEavesdropping \\ &\quad \land\ Correctness \\ &\quad \land\ ExactlyOneAudit \end{aligned}$$

(*
aliceState, * “hasQubit”, “sent”
bobState, * “waiting”, “received”
channelState, * “ready”, “entangled”, “used”, “tampered”
qubitState, * current quantum state (symbolic)
qubitLocation, * “alice”, “bob”, “inChannel”, “eavesdropper”, “lost”
eveInterfered, * TRUE if *Eve* tried to intercept
transferred, * TRUE after teleportation step
auditTrail * Sequence of audit entries *)

* Modification History
* Last modified *Fri Aug* 01 05:46:55 *CEST* 2025 by *tianxiang.lu*
* Created *Fri Aug* 01 05:18:36 *CEST* 2025 by *tianxiang.lu*