Security Proofs using Protocol Composition Logic (PCL)

The goal of this homework is to help you understand and construct proofs using PCL. We begin by summarizing a proof system for First Order Logic (FOL) and relevant rules and axioms of PCL. We then show a proof of an authentication property for a challenge response protocol. Using this proof as a guide, you are required to answer questions about the proof of a related protocol.

First Order Logic

The precondition and postconditions of a PCL modal formula is a First Order logic formula. Reasoning about such formulas requires a proof system for FOL. Without stating the syntax of FOL (assuming familiarity with the basic constructs), we state below the axioms and rules of FOL.

The axioms are

• $\vdash A \lor A \supset A$.
• $\vdash A \supset B \lor A$.
• $\vdash [A \supset B] \supset [C \lor A \supset B \lor C]$.
• $\vdash A \supset \{t/x\}A$, where $t$ is not captured by quantifiers in $A$.
• $\vdash \forall x. [A \lor B] \supset [A \lor \forall x.B]$.

The rules of inference are

• (MP) If we have $\vdash A$ and $\vdash A \supset B$, then we have $\vdash B$.
• (Gen) If $\vdash A$ then $\vdash \forall x.A$.

Very often it is helpful to use certain derived rules of inference. These rules are derived using the axioms and the rule of inference.

• (DR1) If we have $\vdash A_1 \land A_2 \land \ldots \land A_n \supset B$, then we have $\vdash A_1[[[\supset A_2[\supset \ldots \supset [A_n \supset B]\ldots]]]$.
• (DR2) If we have $\vdash A_1[[[\supset A_2[\supset \ldots \supset [A_n \supset B]\ldots]]$, then we have $\vdash A_1 \land A_2 \land \ldots \land A_n \supset B$.
• (TRANS) If we have $\vdash A \supset B$ and $\vdash B \supset C$, then we have $\vdash A \supset C$. 
• (DMP) If we have ⊢ A then we have ⊢ [A ∧ C ⊃ B] ⊃ [C ⊃ B].

• (WEAK) ⊢ A ⊃ A ∨ B.

• (CONTRAWEAK) ⊢ A ∧ B ⊃ A.

• (ALLTOEXISTS) ⊢ ∀x.(A ⊃ B) ⊃ (∃x.A ⊃ ∃x.B).

• (JUMP) Given ⊢ A ⊃ B and ⊢ A ⊃ [B ⊃ C] we have ⊢ A ⊃ C.

We will often use the following equivalences
A ⊃ B ≡ ¬A ∨ B
¬¬A ∧ ¬B ≡ ¬[A ∨ B]
¬A ∨ ¬B ≡ ¬[A ∧ B]

We use {t/x} for substitution operation in which x is substituted by t.

Axioms from PCL

Now we state the axioms from PCL that we use.

<table>
<thead>
<tr>
<th>Axiom</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AA1</td>
<td>⊢ [a]X a</td>
</tr>
<tr>
<td>AA2</td>
<td>⊢ Start(X)[.]X ¬a(X)</td>
</tr>
<tr>
<td>AA3</td>
<td>⊢ ¬Send(X,t)[b]X ¬Send(X,t) if σSend(X,t) ≠ σb for all substitutions σ</td>
</tr>
<tr>
<td>AA4</td>
<td>⊢ [a; ⋯ ; b]X a &lt; b</td>
</tr>
<tr>
<td>AN1</td>
<td>⊢ New(X,x) ∧ New(Y,x) ⊃ X = Y</td>
</tr>
<tr>
<td>C1</td>
<td>⊢ [new x]X ¬Contains(x, SIG_X{[y]})</td>
</tr>
<tr>
<td>C2</td>
<td>⊢ [r := sign (x, X)]X Contains(r, SIG_X{[x, X]})</td>
</tr>
<tr>
<td>VER</td>
<td>⊢ Honest(X) ∧ Verify(Y, SIG_X{[x]}) ∧ X ≠ Y ⊃ ∃X.Send(X, m) ∧ Contains(m, SIG_X{[x]})</td>
</tr>
<tr>
<td>P1</td>
<td>⊢ Persist(X, t)[a]X Persist(X, t) for Persist ∈ {Has, FirstSend, a, Gen}.</td>
</tr>
<tr>
<td>P3</td>
<td>⊢ Persist(t, x)[a]X Persist(t, x) for Persist ∈ {Contains, ¬Contains}. if a does not modify t.</td>
</tr>
<tr>
<td>P4</td>
<td>⊢ c &lt; b[a]X c &lt; b</td>
</tr>
</tbody>
</table>

The rules of inference are as follows:

\[
\frac{\text{Start}(X)[.]X \phi \quad \forall \rho \in Q. \forall P_i \in BS(\rho). \phi [P_i]X \phi}{\text{HON}_Q} \quad \text{Honest}(X) \supset \phi \quad \text{no free variable in } \phi \quad \text{except } X \text{ bound in } [P]X
\]
\[
\begin{align*}
\frac{\theta[P]X\phi \quad \theta[P]X\psi}{\theta[P]X\phi \land \psi} \quad \text{G1} & \quad \frac{\theta[P]X\psi \quad \phi[P]X\psi}{\theta \lor \phi[P]X\psi} \quad \text{G2} \\
\frac{\theta' \supset \theta \quad \theta'[P]X\phi \quad \phi \supset \phi'}{\theta'[P]X\phi} \quad \text{G3} & \quad \frac{\phi}{\theta[P]X\phi} \quad \text{G4}
\end{align*}
\]

\[
\frac{\phi_1[P]X\phi_2 \quad \phi_2[P']X\phi_3}{\phi_1[PP']X\phi_3} \quad \text{SEQ}
\]

**Example Protocol**

\[
A \rightarrow B : m \\
B \rightarrow A : SIG_B\{m, A\}
\]

Figure 1: The protocol as arrows-and-messages

The initiator’s and responder’s program are given below:

\[
\begin{align*}
\text{Init}_{\text{CR}} & \equiv (\hat{Y})[ \\
BS1 & : \text{new } m_1; \\
BS1 & : \text{send } \hat{X}, \hat{Y}, m_1; \\
BS2 & : \text{receive } \hat{Y}, \hat{X}, s; \\
BS2 & : \text{verify } s,(m_1, \hat{X}), \hat{Y}; \\
]_X() \\
\text{Resp}_{\text{CR}} & \equiv ()[ \\
BS3 & : \text{receive } \hat{X}, \hat{Y}, x; \\
BS3 & : r := \text{sign}(x, \hat{X}), \hat{Y}; \\
BS3 & : \text{send } \hat{Y}, \hat{X}, r; \\
]_Y()
\end{align*}
\]

We want to prove the following property for the protocol

\[
\vdash_{Q_{\text{CR}}} \top[\text{Init}_{\text{CR}}]X_{\text{Honest}}(\hat{Y}) \land \hat{Y} \neq \hat{X} \supset \phi_{\text{auth}}
\]

\[
\phi_{\text{auth}} \equiv \exists Y. (\text{Receive}(Y, (\hat{X}, \hat{Y}, m_1)) < \text{Send}(Y, (\hat{Y}, \hat{X}, SIG_Y\{m_1, \hat{X}\})))
\]

**Proof**

We will do the proof in parts. The proof presented below is not purely syntactic since we refer to semantics to obtain certain results (like using all possible substitutions to justify universal quantification)
Part a

In this part, we prove the following formula:

\[ \forall \text{Honest}(\hat{Y}) \land \hat{Y} \neq \hat{X} \supset \exists Y, t. \text{Send}(Y, t) \land \text{Contains}(t, SIG_{\hat{Y}} \{ \hat{m}_1, \hat{X} \}) \]

\[ \forall m. \text{Honest}(\hat{Y}) \land \text{Verify}(X, SIG_{\hat{Y}} \{ \hat{m}_1, \hat{X} \}) \land \hat{Y} \neq \hat{X} \supset \exists Y, t. \text{Send}(Y, t) \land \text{Contains}(t, SIG_{\hat{Y}} \{ \hat{m}_1, \hat{X} \}) \]

\[ \text{DMP, Parta} \]

\[ \exists Y, t. \text{Send}(Y, t) \land \text{Contains}(t, SIG_{\hat{Y}} \{ \hat{m}_1, \hat{X} \}) \supset \] Honest(\hat{Y}) \land \text{Verify}(X, SIG_{\hat{Y}} \{ \hat{m}_1, \hat{X} \}) \land \hat{Y} \neq \hat{X} \supset \exists Y, t. \text{Send}(Y, t) \land \text{Contains}(t, SIG_{\hat{Y}} \{ \hat{m}_1, \hat{X} \})

\[ 7, 8, \text{G3} \]

\[ \forall \text{Honest}(\hat{Y}) \land \hat{Y} \neq \hat{X} \supset \exists Y, t. \text{Send}(Y, t) \land \text{Contains}(t, SIG_{\hat{Y}} \{ \hat{m}_1, \hat{X} \}) \]

Part b

In this part, we prove the following formula:

\[ \forall m. \text{Honest}(\hat{Y}) \land \text{Verify}(X, SIG_{\hat{Y}} \{ \hat{m}_1, \hat{X} \}) \land \hat{Y} \neq \hat{X} \supset \exists Y, t. \text{Send}(Y, t) \land \text{Contains}(t, SIG_{\hat{Y}} \{ \hat{m}_1, \hat{X} \}) \]

\[ \forall m. \text{Honest}(\hat{Y}) \land \text{Verify}(X, SIG_{\hat{Y}} \{ \hat{m}_1, \hat{X} \}) \land \hat{Y} \neq \hat{X} \supset \exists Y, t. \text{Send}(Y, t) \land \text{Contains}(t, SIG_{\hat{Y}} \{ \hat{m}_1, \hat{X} \}) \]

\[ \exists Y, t. \text{Send}(Y, t) \land \text{Contains}(t, SIG_{\hat{Y}} \{ \hat{m}_1, \hat{X} \}) \supset \] Honest(\hat{Y}) \land \hat{Y} \neq \hat{X} \supset \exists Y, t. \text{Send}(Y, t) \land \text{Contains}(t, SIG_{\hat{Y}} \{ \hat{m}_1, \hat{X} \})

\[ 7, 8, \text{G3} \]

\[ \forall \text{Honest}(\hat{Y}) \land \hat{Y} \neq \hat{X} \supset \exists Y, t. \text{Send}(Y, t) \land \text{Contains}(t, SIG_{\hat{Y}} \{ \hat{m}_1, \hat{X} \}) \]

Part c

We use the following abbreviations below:

Let \( A = \text{Honest}(\hat{Y}) \land \hat{Y} \neq \hat{X} \)

\( B = \text{Send}(Y, t) \)

\( C = \text{Contains}(t, SIG_{\hat{Y}} \{ m, \hat{X} \}) \)

\( D = \text{Receive}(Y, (\hat{X}, \hat{Y}, m)) < \text{Send}(Y, (\hat{Y}, \hat{X}, SIG_{\hat{Y}} \{ m, \hat{X} \})) \)

Thus the result of part b then looks like

\[ \forall m. A \supset \{ m \backslash m \} \exists Y, t. B \land C \]

In this part we want to prove

\[ \text{Honest}(\hat{Y}) \supset \forall \hat{X}, t, m. [B \land C \supset D] \]

We can prove this by using the honesty rule. From the formula we need to prove, we get that \( \phi \) should be \( \forall \hat{X}, t, m. [B \land C \supset D] \).
Now for the initiator and responder programs there are three basic sequences (observe that all these basic sequences are run by $\hat{Y}$)

$BS_1 = \text{new } m_1; \text{send } \hat{Y}, \hat{X}, m_1;$
$BS_2 = \text{receive } \hat{X}, \hat{Y}, s; \text{verify } s, (m_1, \hat{Y}), \hat{X};$
$BS_3 = \text{receive } \hat{X}, \hat{Y}, x; r := \text{sign } (x, \hat{X}), \hat{Y}; \text{send } \hat{Y}, \hat{X}, r;$

**Proof Start($X$)**

By axiom AA1

$\text{Start}(Y)[[Y \forall t. \neg \text{Send}(Y, t)]$)

By using WEAK, we have

$\neg \text{Send}(Y, t) \supset \neg \text{Contains}(t, SIG_{\hat{Y}} \{|m, \hat{X}|\}) \lor \neg \text{Send}(Y, t)$

Thus, we can use the last two results to claim that

$\text{Start}(Y)[[Y \forall X, t, m. \neg \text{contain}(t, SIG_{\hat{Y}} \{|m, \hat{X}|\})].$

Or using abbreviation

$\text{Start}(Y)[[Y \forall \hat{X}, t, m. \neg [B \land C].$

Using WEAK we can say that

$\neg [B \land C] \supset [\neg [B \land C] \lor D].$

Using G3 with the last two results we can say that

$\text{Start}(Y)[[Y \forall \hat{X}, t, m. [B \land C \supset D].$

**Proof BS1**

Below is the proof for BS1 with substitution $\{m_1/t\}$

<table>
<thead>
<tr>
<th>Step</th>
<th>Formula</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1</td>
<td>$\top[[\text{new } m_1][[Y \forall \hat{X}, m. \neg \text{Contains}(m_1, SIG_{\hat{Y}} {</td>
</tr>
<tr>
<td>P3</td>
<td>$\forall \hat{X}, m. \neg \text{Contains}(m_1, SIG_{\hat{Y}} {</td>
</tr>
<tr>
<td></td>
<td>$\forall \hat{X}, m. \neg \text{Contains}(m_1, SIG_{\hat{Y}} {</td>
</tr>
<tr>
<td>10, 11, SEQ</td>
<td>$\top [[BS1][[Y \forall \hat{X}, m. \neg \text{Contains}(m_1, SIG_{\hat{Y}} {</td>
</tr>
<tr>
<td>WEAK</td>
<td>$\neg \text{Contains}(m_1, SIG_{\hat{Y}} {</td>
</tr>
<tr>
<td>13, 12, G3</td>
<td>$\top [[BS1][[Y \forall \hat{X}, m. \neg \text{Send}(Y, m_1) \lor \neg \text{Contains}(m_1, SIG_{\hat{Y}} {</td>
</tr>
</tbody>
</table>

Observe that for any wff $X$ we have $\vdash X \supset \top$, thus we have using G3

$\forall \hat{X}, m. \neg \{m_1/t\} [[\text{Send}(Y, t) \land \text{Contains}(t, SIG_{\hat{Y}} \{|m, \hat{X}|\})]] [BS1][[Y$

$\forall \hat{X}, m. \neg \{m_1/t\} [[\text{Send}(Y, t) \land \text{Contains}(t, SIG_{\hat{Y}} \{|m, \hat{X}|\})]] [BS1][[Y$

Below is the proof for BS1 with any substitution $\{m'/t\}$ where $m' \neq m_1$. 

5
Thus, since we have this result for all substitution for \( t \) we can say that
\[
\forall \hat{X}, t, m. \neg \left[ \text{Send}(Y,t) \land \text{Contains}(t, SIG_{\hat{Y}}(\{m, \hat{X}\})) \right][BS1]Y \forall \hat{X}, t, m. \neg \left[ \text{Send}(Y,t) \land \text{Contains}(t, SIG_{\hat{Y}}(\{m, \hat{X}\})) \right].
\]
Or using abbreviation
\[
\forall \hat{X}, t, m. \neg [B \land C] \ [BS1]Y \forall \hat{X}, t, m. \neg [B \land C].
\]

Using WEAK we can say that
\[
\neg [B \land C] \supset \neg [B \land C] \lor D.
\]

Using G3 with the last two results we can say that
\[
\forall \hat{X}, t, m. \neg [B \land C] \ [BS1]Y \forall \hat{X}, t, m. \neg [B \land C] \lor D.
\]

Using P4 we can say that
\[
\forall \hat{X}, t. \text{Receive}(Y, (\hat{X}, \hat{Y}, m)) < \text{Send}(Y, (\hat{Y}, \hat{X}, SIG_{\hat{Y}}(\{m, \hat{X}\}))[BS1]Y \forall \hat{X}, t. \text{Receive}(Y, (\hat{X}, \hat{Y}, m)) < \text{Send}(Y, (\hat{Y}, \hat{X}, SIG_{\hat{Y}}(\{m, \hat{X}\}))).
\]

which is same as
\[
\forall \hat{X}, t. D \ [BS1]Y \forall \hat{X}, t. D.
\]

Using WEAK and the last result we can say that
\[
\forall \hat{X}, t. [B \land C] \lor D \ [BS1]Y \forall \hat{X}, t. [B \land C] \lor D.
\]

Using G2 we can say that
\[
\forall \hat{X}, t. [B \land C] \lor D \ [BS1]Y \forall \hat{X}, t. [B \land C] \lor D.
\]

which is same as
\[
\forall \hat{X}, t. [B \land C] \supset D \ [BS1]Y \forall \hat{X}, t. [B \land C] \supset D.
\]

Proof BS2

We prove here that
\[
\forall \hat{X}, t. [B \land C] \supset D \ [BS2]Y \forall \hat{X}, t. [B \land C] \supset D
\]
Thus, since we have \( \forall X, t, m. B \lor \neg C \)

Now it can be shown that for any other substitution \( \{r/t; x/m\} \)

Below is the proof for BS3 with substitution \( \{r/t; x/m\} \)

Observe that for any wff \( X \) we have \( \vdash X \supset \top \), thus we have using G3 for substitution \( \{r/t; x/m\} \)

Now it can be shown that for any other substitution \( \{s/t; y/m\} \) we have

Thus, since we have \( \{B \land C \supset D\} \) for all substitutions for \( t, m \) we have

\begin{align*}
\text{AA3, SEQ} & \quad \forall X, t, m. \neg B \lor \neg C \quad \text{(22)} \\
\text{WEAK} & \quad \neg B \lor \neg C \quad \text{(23)} \\
22, 23, \text{G3} & \quad \forall X, t, m. \neg B \lor \neg C \\
\text{P3, SEQ} & \quad \forall X, t, m. \neg C \lor \neg B \lor \neg C \\
\text{WEAK} & \quad \neg C \lor \neg B \lor \neg C \\
25, 26, \text{G3} & \quad \forall X, t, m. \neg B \lor \neg C \lor \neg C \\
24, 27, \text{G2} & \quad \forall X, t, m. \neg B \lor \neg C \lor \neg C \\
\end{align*}

\text{Now using similar technique as for BS1 we can conclude that}

\( \forall X, t, m. [B \land C] \supset D \)

\text{Proof BS3}

We prove here that

\( \forall X, t, m. [B \land C] \supset D \)

\text{Remeber BS3 = receive } \hat{X}, \hat{Y}, x; r := \text{sign} (x, \hat{X}), \hat{Y}; \text{send } \hat{Y}, \hat{X}, r;

\text{Below is the proof for BS3 with substitution } \{r/t; x/m\}

\begin{align*}
\text{C2} & \quad \vdash [r := \text{sign} (x, \hat{X})] \land \forall X. \text{Contains}(t, SIG_\hat{Y} \{m, \hat{X}\}) \\
\text{P3, SEQ} & \quad \vdash [BS3]_Y \land \forall X. \text{Contains}(t, SIG_\hat{Y} \{m, \hat{X}\}) \\
\text{AA1} & \quad \vdash [send \hat{Y}, \hat{X}, r] \land \forall X. \text{Send}(Y, t) \\
\text{P1, SEQ} & \quad \vdash [BS3]_Y \land \forall X. \text{Send}(Y, t) \\
\text{AA4} & \quad \vdash [BS3]_Y \\
& \quad \forall X. \text{ contain}(t, SIG_\hat{Y} \{m, \hat{X}\}) \\
30, 32, \text{G1} & \quad \vdash [BS3]_Y \land \forall X. \text{ Send}(Y, t) \land \forall X. \text{ Contains}(t, SIG_\hat{Y} \{m, \hat{X}\}) \\
\end{align*}

Observe that for any wff \( X \) we have \( \vdash X \supset \top \), thus we have using G3 for substitution \( \{r/t; x/m\} \)

which is same as \( \{r/t; x/m\} \)

Now it can be shown that for any other substitution \( \{s/t; y/m\} \) we have

So for this substitution \( \{s/t; y/m\} \) we can use same steps as for BS1 to get

Thus, since we have \( \{B \land C \supset D\} \) for all substitutions for \( t, m \) we have

\begin{align*}
\forall X, t, m. [B \land C] \supset D \\
\end{align*}
Honesty Result

Now we can use Honesty Rule and claim that
\[
\text{Honest}(\hat{Y}) \supset \forall \hat{X}, t, m.[B \land C \supset D]
\]

Part d

Now using CONTRAWEAK we get
\[
\text{Honest}(\hat{Y}) \land \hat{Y} \neq \hat{X} \supset \text{Honest}(\hat{Y})
\]

Using TRANS with the last result and the result of the honesty rule we get
\[
\text{Honest}(\hat{Y}) \land \hat{Y} \neq \hat{X} \supset \forall \hat{X}, t, m.[B \land C \supset D]
\]

Thus, we have by putting in the formulas for \(B, C\) and \(D\)
\[
\text{Honest}(\hat{Y}) \land \hat{Y} \neq \hat{X} \supset \forall \hat{X}, t, m.[\text{Send}(Y, t) \land \text{Contains}(t, SIG_{\hat{Y}}\{m, \hat{X}\})) \supset (\text{Receive}(Y, (\hat{X}, \hat{Y}, m)) < \text{Send}(Y, (\hat{Y}, \hat{X}, SIG_{\hat{Y}}\{m, \hat{X}\}))]
\]

Using the abbreviations we can write the above result as
\[
A \supset \forall \hat{X}, t, m.[B \land C \supset D]
\]

Part e

Since the honesty result is quantified over all \(\hat{X}\) we can instantiate it for our agents also (which has the name \(\hat{X}\)). Also since \(Y\) is free we can universally quantify the formula with \(Y\). Thus, we get
\[
A \supset \forall Y, t, m.[B \land C \supset D]
\]

Now using ALLTOEXISTS we get
\[
\forall m.(\forall Y, t.[B \land C \supset D] \supset [\exists Y, t.[B \land C] \supset \exists Y, t.D])
\]

Using TRANS with the last result and Part d we get
\[
A \supset \forall m.\exists Y, t.[B \land C] \supset \exists Y, t.D
\]

Now we know from part b that
\[
\top[\text{Init}_{\text{CR}}].A \supset \{m_1/m\}\exists Y, t. B \land C
\]

Using JUMP with the last result and Part b we get
\[
\top[\text{Init}_{\text{CR}}].A \supset \{m_1/m\}\exists Y.D \text{ (note } t \text{ does not occur in } D)
\]

which is same as
\[
\top[\text{Init}_{\text{CR}}].\text{Honest}(\hat{Y}) \land \hat{Y} \neq \hat{X} \supset \exists Y. (\text{Receive}(Y, (\hat{X}, \hat{Y}, m_1)) < \text{Send}(Y, (\hat{Y}, \hat{X}, SIG_{\hat{Y}}\{m_1, \hat{X}\}))]
\]
The homework problem pertains to a related protocol $Q_{WCR}$ given below

\[
X \rightarrow Y : m \\
Y \rightarrow X : \text{SIG}_B\{m\}
\]

The initiator's and responder's programs are given below:

\[
\text{Init}_{WCR} \equiv (\hat{Y})[\begin{array}{l}
\text{new } m; \\
\text{send } \hat{X}, \hat{Y}, m; \\
\text{receive } \hat{Y}, \hat{X}, s; \\
\text{verify } s, (m)\hat{Y}; \\
\end{array}]x() \\
\text{Resp}_{WCR} \equiv ([])[\begin{array}{l}
\text{receive } \hat{X}, \hat{Y}, x; \\
r := \text{sign}(x), \hat{Y}; \\
\text{send } \hat{Y}, \hat{X}, r;
\end{array}]y()
\]

Problem a

Consider the following theorem for the protocol described above.

\[
\vdash_{Q_{WCR}} T[\text{Init}_{CR}]_X^{\text{Honest} (\hat{Y}) \land \hat{Y} \neq \hat{X} \supset \phi_{auth}.} \\
\phi_{auth} \equiv \exists Y. (\text{Receive}(Y, (X, \hat{Y}, m)) < \text{Send}(Y, (\hat{Y}, \hat{X}, \text{SIG}_Y\{m\})))
\]

1. Show an attack demonstrating that $Q_{WCR}$ does not have this property $\phi$.

2. Examine the example proof of $Q_{CR}$ and indicate which part of the proof breaks for $Q_{WCR}$ (part a, part b or part c). Indicate a specific line in the proof that can no longer be proved and explain informally why that is the case.

Problem b

Now prove the following theorem for $Q_{WCR}$ described above.

\[
\vdash_{Q_{CW_R}} T[\text{Init}_{CR}]_X^{\text{Honest} (\hat{Y}) \land \hat{Y} \neq \hat{X} \supset \phi_{auth}.} \\
\phi_{auth} \equiv \exists Y. \exists \hat{Z}. (\text{Receive}(Y, (\hat{Z}, \hat{Y}, m)) < \text{Send}(Y, (\hat{Y}, \hat{Z}, \text{SIG}_Y\{m\})))
\]

You can use the proof of $Q_{CR}$ as a guide.