第 5 章

基于行为模型的密码协议验证

本章用行为模型(action model)来扩展认知逻辑以构建语言来描述并验证密码协议。本章还是采用第 4 章的实例作为分析验证的例子。

5.1 协议的语言 $\mathcal{L}^{A,B}_{\mathrm{Cryp}}$

本节用行为模型来描述这个实例,令语言为 $\mathcal{L}^{A,B}_{\mathrm{Cryp}}$,其中 Cryp 表示密码学(cryptography),A 是协议全体主体集,$B \subseteq A$ 是主体集中一个子集,表示在认知状态中将被分析的参与这个协议的主体。这个语言中的命题由 has、const、tg 构成,has 表示主体拥有的消息,const 表示主体可以从自身的信息集构造的消息,tg 表示为密码协议中已经完成的行为做标记。用 表示行为集。

5.1.1 协议语言 $\mathcal{L}^{A,B}_{\mathrm{Cryp}}$ 的语法

本章对协议中的消息集 的定义沿用定义 4.1,即 $m ::= a \mid n \mid k \mid m_k \mid (m, m)(m \in$ $)$。

定义 5.1:本协议基本命题 在这个密码协议系统中,用 Φ^{A}_{Cryp} 作为基本命题 p 的集合,基本命题 p 定义为

$$p ::= \mathrm{has}_a m \mid \mathrm{const}_a m \mid \mathrm{tg}(\sigma)$$

其中,$a \in A$,$m \in$,$\sigma \in$ 。$\mathrm{has}_a m$ 表示主体 a 拥有消息 m,$\mathrm{const}_a m$ 表示主体 a 从自己的信息集构造 m,$\mathrm{tg}(\sigma)$ 表示行为 σ 被标记。令 Φ_I,$\Phi_{\bar{I}}$,Φ_{tg} 是 Φ^{A}_{Cryp} 的子集,分别表示上述 3 种命题的集合。

下面定义行为模型。根据文献[160]的思想,一个行为的执行需要的条件称为前提条件(precondition),没有相应的前提条件,这个行为是不能被执行的。在这个系统中,所有的前提条件属于 Φ^{A}_{Cryp},它是语言 $\Phi^{A,B}_{\mathrm{Cryp}}$ 的一部分。一个行为执行后成立的命题称为后置条件(postcondition),后置条件表明行为执行后知

识的变化，后置条件分为两部分，一个是 Pos_I 表明主体信息集的变化，另一个是 $\mathrm{Pos}_{\mathrm{AL}}$ 表明行为标记的变化（记录主体完成的行为）。基于逻辑语言 $\mathcal{L}_{\mathrm{Cryp}}^{A,B}$，一个行为模型是一个元组 $\mathfrak{A}=(\quad,\sim_a,\mathrm{Pre},\mathrm{Pos}_I,\mathrm{Pos}_{\mathrm{AL}})$，其中 $\quad$ 是一个非空的有限的行为集，对所有的 $a\in B$，$\sim_a$ 是一个等价关系。Pre：$\quad\to\Phi_{\mathrm{Cryp}}^{A}$ 为每一个行为指派一个前提条件。应用文献[160]的思想处理后置条件，函数 $\Phi\to\quad$ 是对 $\quad$ 的一个替换，是基本的逻辑语言到它的变体的一个映射。SUB 是 substitution 的缩写，SUB( )被看作从 Φ（命题）到 （语言）的一个替换集。因此，Pos_I：$\quad\to\mathrm{SUB}(\Phi_{\mathrm{Cryp}}^{A,B})$，后置条件是语言 $\mathcal{L}_{\mathrm{Cryp}}^{A,B}$ 的一个替换，对任意的 $p\in\Phi_I$，$\sigma\in\quad$，有性质 $\mathrm{Pos}_I(\sigma)(p)\in\Phi_I\cup\{\quad,\}$。$\mathrm{Pos}_{\mathrm{AL}}$：$\quad\to\mathrm{SUB}(\Phi_{\mathrm{Cryp}}^{A,B})$，对任意的 $p\in\Phi_{\mathrm{AL}}$，$\sigma\in\quad$，有 $\mathrm{Pos}_{\mathrm{AL}}(\sigma)(p)\in\Phi_{\mathrm{AL}}\cup\{\quad,\}$。用“$m\in I_a$（$I_a$ 表示 a 的信息集）”替换“$\mathrm{has}_a m$”映射到 $\quad$，同时，在 σ 行为执行后消息 m 增加到 a 的信息集。用“σ^+”来标记当前行为对替换映射 $\mathrm{tg}(\sigma)$ 到 $\quad$，同样地，用“σ^-”来标记之前的行为对替换映射 $\mathrm{tg}(\sigma)$ 到 $\quad$。在后面的分析过程中，将用这些替换来形式化所有的后置条件。

定义 5.2：本协议语言 $\mathcal{L}_{\mathrm{Cryp}}^{A,B}$ 的语法 给定主体集 A 和基本命题集 Φ_{Cryp}^{A}，协议语言 $\mathcal{L}_{\mathrm{Cryp}}^{A,B}$ 的语法归纳定义为

$$\varphi::=\quad\mid p\mid\neg\varphi\mid\varphi\vee\varphi\mid K_a\varphi\mid[\alpha]\varphi$$
$$\alpha::=(\mathfrak{A},\sigma)$$

其中，$p\in\Phi_{\mathrm{Cryp}}^{A}$，$a\in\mathfrak{A}$，$\sigma$ 是行为模型 $\mathfrak{A}$ 中的一个行为。$[\mathfrak{A},\sigma]\varphi$ 意思是在 $\mathfrak{A}$ 中的行为 σ 执行后，φ 成立。

5.1.2 协议语言 $\mathcal{L}_{\mathrm{Cryp}}^{A,B}$ 的语义

语言 $\mathcal{L}_{\mathrm{Cryp}}^{A,B}$ 的模型 $\mathfrak{M}$ 是一个元组

$$\mathfrak{M}=(W,\{R_a\}_{a\in B},I,\mathrm{AL})$$

其中，W 是一个非空的可能世界集，R_a 是对所有的 $a\in B$ 在 W 上的二元关系。I 是信息集，$I_{w,a}$ 表示在世界 w，主体 a 的信息集，也就是说 $I:W\times\quad\to\mathcal{P}(\quad)$。

AL 表示行为标签，即 $\mathrm{AL}:W\to\mathcal{P}(\quad)$。对任意的 $\sigma\in\quad$，$\mathrm{tg}(\sigma)$ 意味着在行为集 $\quad$ 的行为 σ 已经被标记。I 和 AL 是对应的基本命题的值。若 $m\in I_a$，则 $\mathrm{has}_a m$ 成立。m 是 a 的拥有集的消息，可以是通过接收得到的也可以是初始分配的，消息 m 也可以由主体从它的信息集中的信息构造的，构造规则遵循第 4 章介绍的密码学构造规则，即

$$\frac{m\ k}{m_k}\qquad\frac{m_k\ k}{m}\qquad\frac{mm'}{(m,m')}\qquad\frac{(m,m')}{m}\qquad\frac{(m,m')}{m'}$$

令协议语言 $\mathcal{L}_{\mathrm{Cryp}}^{A,B}$ 的模型为 $\mathfrak{M}$，基本命题的语义如下：

$\mathfrak{M},w \quad \mathrm{has}_a m$ 当且仅当 $m \in I_{w,a}$；

$\mathfrak{M},w \quad \mathrm{const}_a m$ 当且仅当 $m \in \overline{I_{w,a}}$；

$\mathfrak{M},w \quad \mathrm{tg}(\sigma)$ 当且仅当 $\sigma \in \mathrm{AL}(w)$；

第一条是说如果模型在世界 w 满足主体 a 拥有消息 m，当且仅当，消息 m 属于 a 在世界 w 的信息集。第二条说主体 a 可以构造消息 m 在 $(\mathfrak{M},w)$，当且仅当 m 可以从他的信息集 $I_{w,a}$ 推导，“$m \in \overline{I_{w,a}}$”表示 m 属于集合 $I_{w,a}$ 的推导集（$\overline{I_{w,a}}$ 表示从集合 $I_{w,a}$ 推导出来的信息集）。第三条表明，$\mathrm{tg}(\sigma)$ 在 $(\mathfrak{M},w)$ 成立，当且仅当 σ 在 $(\mathfrak{M},w)$ 被标记。

更新模型令协议语言 $\mathcal{L}_{\mathrm{Cryp}}^{A,B}$ 的模型为 $\mathfrak{M}$，$\mathfrak{A}$ 是行为模型，更新模型

$$\mathfrak{M}\circ\mathfrak{A}=(W',\{R'_a\}_{a\in B},I',\mathrm{AL}')$$

被定义为

$$W'=\{\langle w,\sigma\rangle \mid \mathfrak{M},w \quad \mathrm{Pre}(\sigma)\}$$
$$R'_a=\{\langle w,\sigma\rangle,\langle v,\sigma'\rangle \mid w\ R'_a\ v \text{ 和 } \sigma\sim_a\sigma'\}$$
$$I'_{(\langle w,\sigma\rangle,a)}=\{m \mid \mathfrak{M},w \quad \mathrm{Pos}_I(\sigma)(\mathrm{has}_a m)\}$$
$$\mathrm{AL}'_{(\langle w,\sigma\rangle)}=\{\beta \mid \mathfrak{M},w \quad \mathrm{Pos}_{\mathrm{AL}}(\sigma)(\mathrm{tg}(\beta))\}$$

定义 5.3：本协议语言 $\mathcal{L}_{\mathrm{Cryp}}^{A,B}$ 的语义 给定主体集 A 和基本命题集 Φ_{Cryp}^{A}，协议模型为 $\mathfrak{M}=(W,\{R_a\}_{a\in B},I,\mathrm{AL})$ 且状态 $w\in W$，本协议语言 $\mathcal{L}_{\mathrm{Cryp}}^{A,B}$ 的语义定义如下：

$\mathfrak{M},w$ 当且仅当 $\mathfrak{M},w$ ；

$\mathfrak{M},w \quad \neg\varphi$ 当且仅当 $\mathfrak{M},w \quad \varphi$；

$\mathfrak{M},w \quad \varphi\vee\psi$ 当且仅当 $\mathfrak{M},w \quad \varphi$ 或者 $\mathfrak{M},w \quad \psi$；

$\mathfrak{M},w \quad \mathbf{K}_a\varphi$ 当且仅当对任意一个 $w'\in W$，若 $w\,R_a w'$，则 $\mathfrak{M},w' \quad \varphi$；

$\mathfrak{M},w \quad [\mathfrak{A},\sigma]\varphi$ 当且仅当若 $\mathfrak{M},w \quad \mathrm{Pre}(\sigma)$，则 $\mathfrak{M}\otimes\mathfrak{A},\langle w,\sigma\rangle \quad \varphi$。

5.2 协议形式化

5.2.1 形式化密码协议中的基本问题

1. 协议形式化描述形式

这里用 Crypto 来表示该密码协议的行为模型。事实上协议的运行是一系列动作的执行。在密码学中，协议被描述为这样的形式：

$a\rightarrow b$：m 表示主体 a 发送消息 m 给 b， 其中，$m\in M$

2. 实例化

行为模式是协议执行中的一个重要部分。通常用 instatiation θ 实例化行为模式，θ 为任意的一个实例。instatiation θ 是一个从协议参数到它们各自的域的映射。一个协议的执行有几个实例的相互交错。在该系统中，应用 Θ 来表示实例集，协议的参数是有限的，因此 Θ 集的元素也是有限的。

3. 网络环境

参照文献[161]，假定该协议的网络由输入缓冲器(input buffer)和输出缓冲器(output buffer)构成。将这两部分看作两个特殊的主体 In 和 Out。可信任的主体消息仅能发送给 In，攻击者或入侵者能够窃听 In 的信息。可信主体仅能接收来自 Out 的消息。

4. 验证模型

验证模型是该协议要达到的目标模式。在协议运行结束后，目标公式 ϕ（$\phi \in \Phi_{\mathrm{Cryp}}^{A,B}$）成立，形式化验证模型如下：

$$\mathfrak{M} \quad \bigwedge_{\theta \in \Theta} [\mathrm{Crypto}_{\mathrm{Intr}}, \sigma(\theta)] \phi(\theta)$$

其中，$\mathfrak{M}$ 是之前定义的模型，包括所有初始假设条件和所有主体的初始认知信息。$\mathrm{Crypto}_{\mathrm{Intr}}$ 表示行为模型，这个模型中的行为包括入侵者的行为。Intr 表示入侵者(intruder)。σ 是行为模型 A 中的行为，通常是行为序列中的最后一个。ϕ 是 $\Phi_{\mathrm{Cryp}}^{A,B}$ 中的公式，或者是静态认知公式或者是命题公式。

$$\bigwedge_{\theta \in \Theta} [\mathrm{Crypto}_{\mathrm{Intr}}, \sigma(\theta)] \phi(\theta)$$

表示包括入侵者的行为的模型 $\mathrm{Crypto}_{\mathrm{Intr}}$ 中所有的行为执行完成之后，公式 ϕ 成立。这是协议的目标模型的表达式。

5.2.2 形式化行为模型

在协议的运行中语言模型的变化依赖于行为的执行。也就是说，行为的执行导致模型的变化。因此，首先给出行为模型。前面定义了初始化模型 $\mathfrak{M}$ 和行为模型 $\mathrm{Crypto}_{\mathrm{Intr}}$。假定 Ag 表示协议中主要被分析的主体集，入侵者(intruder) T（$T \in Ag$）执行入侵行为。所以，在这个系统中，主体集 $A = Ag \cup \{\mathrm{In}, \mathrm{Out}\}$ 和 $B = Ag$。入侵者的行为和协议的行为要求是根据入侵者模型和来源于在 $\mathrm{Crypto}_{\mathrm{Intr}}$ 模型中行为集　的协议规定的行为。

在协议中，$a \rightarrow b$：m 表示 a 发送消息 m 给 b。这个行为分成'send'$(\sigma)a \rightarrow \mathrm{In}$：$m$ 和'receive'$(\delta)\mathrm{Out} \rightarrow b$：$m$ 两部分。执行这个行为的前提是 a 可以从他的信息集构造 m：$\mathrm{Pre}(\sigma) = \mathrm{const}_a\, m$。行为 σ 的后置条件是 $\mathrm{Pos}_I(\sigma) = m \in I_{\mathrm{In}}$。用

σ^+，σ^-来标记刚刚完成的行为和这个行为之前的行为。同样地，行为 δ 的前提条件为 $\mathrm{Pre}(\delta)=\mathrm{has}_{\mathrm{out}}m$。规定缓冲器本身不能构造新的信息。$\delta$ 的后置条件为 $\mathrm{Pos}_I(\delta)=m\in I_b$。

在这个网络模型中，假定入侵者可能窃听所有缓冲器的信息。因此，入侵者 T 的行为是 In→T：m 或者 T→Out：m。也就是说，一方面入侵者可以从输入缓冲器获取信息(take m)，另一方面他可以把信息放入输出缓冲器(fake m)。这个行为描述如表 5.1 所示。

表 5.1 入侵者 T 的行为模型

Action	Direction	Message	Pre	Pos_I	$\mathrm{Pos}_{\mathrm{AL}}$
take m	In→T	m	$\mathrm{has}_{\mathrm{In}}m$	$m\in I_T$	—
fake m	T→Out	m	$\mathrm{const}_T m$	$m\in I_{\mathrm{Out}}$	—

在这个系统中，主体只能区分他自己完成的行为，别的主体的行为不可区分的。用$\sim_a$来表示任意主体 a 不可区分的行为，$\sim_T$ 表示入侵者不可区分的行为。协议的模型 $\mathfrak{M}=(W,\{R_a\}_{a\in B},I,\mathrm{AL})$的初始状态描述如下。

W 是一个非空的可能世界集。

I 是主体的信息集。一个主体的信息集总是基于一个确定的世界。因此，主体 a 和他的信息集 I 定义一个世界 w，通常地，写作 $I_{(w,a)}$。在初始状态，规定缓冲器是空的，因此对所有的 $w\in W$，在初始状态有 $I_{(w,\mathrm{In})}=I_{(w,\mathrm{Out})}=\varnothing$。

R_a 如果 wR_av，当且仅当 $I_{(w,a)}=I_{(v,a)}R_a$ 表示对主体 a 来说是等价关系，a 不能区分 w 和 v。

AL 在初始状态，对所有的 $w\in W$，令 $\mathrm{AL}(w)=\varnothing$。

在后面分析具体协议时，将应用上面的形式化方法。

5.3 协议分析

沿用第 4 章的例子。在一个不安全的网络中，甲想发送给乙一个秘密消息 m。他们只有自己的密钥。假定甲作为发送者(S)，乙作为接收者(R)。发送者有自己的密钥 k_s，接收者有自己的密钥 k_r。他们只能解密自己加密的数据。协议描述如下：

(1) S→R：m_s

(2) R→S：m_{sr}

(3) $S \rightarrow R: m_r$

在第(1)步,发送者用 k_s 加密 m 得到 $\{m\}_{k_s}$,为了简洁,写作 m_s。发送者将 m_s 发送给接收者。接收者收到后,用 k_r 加密 m_s 得到 m_{sr}。再把 m_{sr} 返回给发送者,发送方解密 m_{sr} 得到 m_r 并发送到接收者。接收者可以解密 m_r 并得到 m。最后,m 从 S 传输到 R。应用的加密有可交换的性质,即 $m_{sr}=m_{rs}$(加密信息时密钥的使用顺序的改变不改变加密结果)。这里,密钥可以是对称的,也可以是非对称的公私钥对密钥。下面形式化这个协议。在协议中,消息集 $M=\{k_s,k_r,m,m_s,m_{sr},m_r\}$,$Ag=\{S,R,T\}$,其中 S 是发送者,R 是接收者,T 是入侵者。协议的全体主体集为 $A=\{S,R,T,\mathrm{In},\mathrm{Out}\}$,着重分析的协议参与者集合 $B=Ag=\{S,R,T\}$。首先给出初始模型图 5.1,然后根据协议行为的执行的运行过程形式化协议。在初始状态,只有 S 有信息 m 其他人没有 m,初始模型中表明了哪一个主体拥有 m。根据 $I_{w,S}$,$I_{w,R}$,$I_{w,T}$,如果主体在那个世界有 m 就出现在那个世界。在图 5.1 中,实线表示这两端的世界对 S 是可以区分的(其余是不能区分的),虚线表示两端的世界对 T 是可以区分的,点线表示两端的世界对 R 是可以区分的。因此,在初始状态满足:$\mathfrak{M},S \quad \mathrm{has}_S m \wedge \neg \mathrm{has}_R m \wedge \neg \mathrm{has}_T m$。

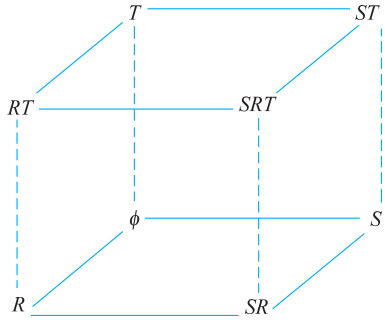

图 5.1 协议的初始模型

协议的行为模型形式化如表 5.2 所示。

表 5.2 协议的行为模型形式化

Action	Direction	Message	Pre	Pos_I	Pos_{AL}
σ_1	$S \rightarrow \mathrm{In}$	m_s	$\mathrm{const}_S m_s$	$m_s \in I_{\mathrm{In}}$	σ_1^+
δ_1	$\mathrm{Out} \rightarrow R$	m_s	$\mathrm{has}_{\mathrm{Out}} m_s$	$m_s \in I_R$	δ_1^+
σ_2	$R \rightarrow \mathrm{In}$	m_{sr}	$\mathrm{const}_R m_{sr}$	$m_{sr} \in I_{\mathrm{In}}$	δ_1^-, σ_2^+
δ_2	$\mathrm{Out} \rightarrow S$	m_{sr}	$\mathrm{has}_{\mathrm{Out}} m_{sr}$	$m_{sr} \in I_S$	δ_2^+
σ_3	$S \rightarrow \mathrm{In}$	m_r	$\mathrm{const}_S m_r$	$m_r \in I_{\mathrm{In}}$	δ_2^-, σ_3^+
δ_3	$\mathrm{Out} \rightarrow R$	m_r	$\mathrm{has}_{\mathrm{Out}} m_r$	$m_r \in I_R$	δ_3^+

如表 5.2 所示,行为 σ_1 表示 S 将消息 m_s 发送到 In,前提条件是 S 能够构

造 m_s，后置条件是 m_s 属于 In，同时标记 σ_1 这个行为。第 2 行 δ_1 表示 R 从 Out 接收到消息 m_s，前提是 Out 有消息 m_s，这个行为执行后 R 有消息 m_s，同时标记 δ_1。第 3 行的“δ_1^-，σ_2^+”中“δ_1^-”，表示 R 执行的当前行为是 σ_2，之前的一个行为是 δ_1。这里将协议参与主体 S，R 的当前行为和前一个行为都做了标记。

表 5.3 中添加了来自入侵者（T）的操作。假设入侵者是一个弱的入侵者。除了窃听他无法构造任何信息，因为没有密钥，所以只能从缓冲区中接收所有消息并传输到输出缓冲器。

表 5.3 包括入侵者行为的行为模型

Action	Direction	Message	Pre	Pos_I	Pos_{AL}
σ_1	$S\rightarrow$In	m_s	$const_S m_s$	$m_s \in I_{In}$	σ_1^+
take m_s	In$\rightarrow T$	m_s	$has_{In} m_s$	$m_s \in I_T$	—
fake m_s	$T\rightarrow$Out	m_s	$has_T m_s$	$m_s \in I_{Out}$	—
δ_1	Out$\rightarrow R$	m_s	$has_{Out} m_s$	$m_s \in I_R$	δ_1^+
σ_2	$R\rightarrow$In	m_{sr}	$const_R m_{sr}$	$m_{sr} \in I_{In}$	δ_1^-，σ_2^+
take m_{sr}	In$\rightarrow T$	m_{sr}	$has_{In} m_{sr}$	$m_{sr} \in I_T$	—
fake m_{sr}	$T\rightarrow$Out	m_{sr}	$has_T m_{sr}$	$m_{sr} \in I_{Out}$	—
δ_2	Out$\rightarrow S$	m_{sr}	$has_{Out} m_{sr}$	$m_{sr} \in I_S$	δ_2^+
σ_3	$S\rightarrow$In	m_r	$const_S m_r$	$m_r \in I_{In}$	δ_2^-，σ_3^+
take m_r	In$\rightarrow T$	m_r	$has_{In} m_r$	$m_r \in I_T$	—
fake m_r	$T\rightarrow$Out	m_r	$has_T m_r$	$m_r \in I_{Out}$	—
δ_3	Out$\rightarrow R$	m_r	$has_{Out} m_r$	$m_r \in I_R$	δ_3^+

5.4 协议验证

5.4.1 协议的目标模型

在初始状态，S 和 R 有自己的密钥，但只有 S 才有秘密消息 m。协议目标是所有动作执行完成后，R 有秘密消息 m，而 T 没有。因此，得出目标模型。

目标 1：在最后一个行为 δ_3 执行后，R 有秘密消息 m。

$$\mathfrak{M} \quad \bigwedge_{\theta\in\Theta}[\mathrm{Crypto}_{\mathrm{Intr}},\delta_3(\theta)]\mathrm{K}_{Ag}\,\mathrm{const}_R m(\theta)$$

目标 2：在初始状态 T 没有 m，在最后一个行为 δ_3 执行后，T 仍然没有 m。

$$\mathfrak{M} \quad \bigwedge_{\theta\in\Theta}\neg\,\mathrm{has}_T m(\theta)\rightarrow[\mathrm{Crypto}_{\mathrm{Intr}},\delta_3(\theta)]\mathrm{K}_{Ag}\neg\,\mathrm{const}_T m(\theta)$$

如果协议满足目标 1 和目标 2，那么该协议是安全的。

5.4.2 协议的验证

命题 1：对于任何一组消息项　，以及任意秘密消息 m：没有密钥 k，如果 $m\notin$ ¯，则 $m\notin\overline{\boldsymbol{m}_k\cup}$。

从构造规则来看，如果主体有 m_k 和相应的密钥 k，则可以构造 m。没有密钥 k，如果 m 不能从　推导（能从　推导得出的集合表示为 ¯），则即使 m_k 并到　集，还是不能推导得出 m，因为缺少前提密钥 k。根据这个命题，T 不能计算秘密消息 m，因为他的消息都来自输入缓冲器，从表 5.3 的 Pos_I 列可以看出，他没有相应的密钥 k。在这个系统中，主体的消息集的元素总是增加而不是减少的。因此得出命题 2。

命题 2：对任意消息 m 和任意主体 a，有

$$\mathfrak{M} \quad \mathrm{const}_a m\rightarrow[\mathrm{Crypto}_{\mathrm{Intr}}]\mathrm{const}_a m$$

命题 3：目标 2 在协议的运行过程中总是真的。

在初始状态，只有 S 有消息 m，其他人没有 m。当然 T 不可能有 m，因为协议还没有运行，什么行为也没有做。

现在证明目标 2 在协议的运行过程中总是真的。

假设存在一个世界 w 不满足目标 2，

$$\mathfrak{M},w \quad \neg\,\mathrm{has}_T m\rightarrow[\mathrm{Crypto}_{\mathrm{Intr}}]\neg\,\mathrm{const}_T m$$

如果上面这个公式成立，那么就存在一个动作序列 $\sigma_1,\sigma_2,\cdots,\sigma_n(\sigma_i\in$　），使得

$$\mathfrak{M},w \quad \neg\,\mathrm{has}_T m\wedge[\mathrm{Crypto}_{\mathrm{Intr}},\sigma_1]\cdots[\mathrm{Crypto}_{\mathrm{Intr}},\sigma_n]\mathrm{const}_T m$$

然而，从表 5.3 可以看到，在任何一个状态，T 都没有 m，所以

$$\mathfrak{M},w \quad \neg\,\mathrm{has}_T m\wedge[\mathrm{Crypto}_{\mathrm{Intr}},\sigma_1]\cdots[\mathrm{Crypto}_{\mathrm{Intr}},\delta_3]\neg\,\mathrm{const}_T m$$

因此，假设是不成立的。

入侵者仅能从输入缓冲器得到信息。如果 $m\in I_{\mathrm{In}}$，那么 $m\in I_T$。从表 5.2 或表 5.3 可以列出输入缓冲器的信息集

$$\bigcup_{1\leqslant i\leqslant n} I_{(w_i,I_n)}=\{m_s,m_{sr},m_r\}$$

因此，T 拥有的消息都是加密数据，没有相应的密钥 k，他不能计算并得到秘密消息 m。因此目标 2 是满足的。

命题 4：目标 1 在初始状态不成立，在协议的最后一个行为 δ_3 完成后，目标 1 成立。

证明：在初始状态，R 没有 m，R 只有 k_r。协议的所有行为执行后，根据表 5.3，R 的信息集为

$$\bigcup_{1\leqslant i\leqslant n} I_{(w_i,R)} = \{m_s, m_{sr}, m_r\}$$

因此，R 有 k_r 和 m_r，根据构造规则，R 可以构造出 m，即 $\mathrm{const}_R\, m$。因此，协议的所有行为执行后，得到下式：

$$\mathfrak{M}\quad [\sigma_1][\mathrm{take}][\mathrm{fake}][\delta_1][\sigma_2][\mathrm{take}][\mathrm{fake}][\delta_2][\sigma_3][\mathrm{take}][\mathrm{fake}][\delta_3]\mathrm{const}_R m$$

因此，目标 1 和目标 2 得证。此协议是满足安全要求的。

5.5 本章小结

本章应用文献[75,160]的思想用行为模型扩展认知逻辑形成动态认知逻辑，描述、分析并验证一个具体的密码协议。这个协议是两个主体，要在一个不安全的网络中传送一个秘密消息，它们仅有自己的密钥，只能解密自己加密的消息。本章给出了描述这个协议的语言的语法和语义。用行为模型来刻画协议的行为，行为的执行导致模型的变化，更新模型描述了模型的转换。精确地详细地模式化协议的每一步。从实际意义上来说，逻辑表示就是逻辑分析。根据安全要求，给出协议的安全目标，通过分析和证明，这个协议满足预设的目标，这个协议是安全的。