软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2011,22(3):534−557 [doi: 10.3724/SP.J.1001.2011.03732]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

时间相关密码协议逻辑及其形式化语义*

雷新锋[1,2+], 刘 军[2], 肖军模[2]

[1](中国科学院 软件研究所 信息安全国家重点实验室,北京 100190)

[2](解放军理工大学 通信工程学院,江苏 南京 210007)

Time-Dependent Cryptographic Protocol Logic and Its Formal Semantics

LEI Xin-Feng[1,2+], LIU Jun[2], XIAO Jun-Mo[2]

[1](State Key Laboratory of Information Security, Institute of Software, The Chinese Academy of Sciences, Beijing 100190, China)

[2](Institute of Communications Engineering, PLA University of Science and Technology, Nanjing 210007, China)

+ Corresponding author: E-mail: leixinfeng@is.iscas.ac.cn

Lei XF, Liu J, Xiao JM. Time-Dependent cryptographic protocol logic and its formal semantics. *Journal of Software*, 2011,22(3):534−557. http://www.jos.org.cn/1000-9825/3732.htm

Abstract: In cryptographic protocols, the agent's epistemic and doxastic states are changeable over time. To model these dynamics, a time-dependent cryptographic protocol logic is proposed. Our logic is based on the predicate modal logic and the time factor can be expressed in it by invoking a time variable as a parameter of predicates and modal operators. This makes it possible to model every agent's actions, knowledges and beliefs at different time points. We also give the formal semantics of our logic to avoid the ambiguity of its language and make the logic sound. The semantics is based on the kripke structure and the possible world in it is built both on the local world of agent and the specific world of time. This makes every possible world can give a global view of each point of the protocol. Our logic provides a flexible method for analyzing the cryptographic protocols, especially the time-dependent cryptographic protocols, and increases the power of the logical method for analyzing protocols.

Key words: cryptographic protocol; time-dependent; predicate modal logic; formal semantics

摘 要: 在密码协议中,主体的认知与信仰状态是随时间推移而不断变化的.为了在协议分析中体现这种动态性,提出一种时间相关密码协议逻辑.该逻辑基于谓词模态逻辑,通过在谓词及模态词中引入时间参数以体现时间因素,使得逻辑可表达各个主体在协议不同时间点的行为、知识及信仰.给出该逻辑的形式化语义,在避免逻辑语言二义性的同时保证了逻辑的可靠性.该语义基于Kripke结构,将可能世界建立在主体局部世界与时间局部世界的基础上,使得任一可能世界能够反映协议的一个可能的全过程.该逻辑为密码协议,特别是时间相关密码协议提供了灵活的分析方法,增强了基于逻辑方法的协议分析能力.

关键词: 密码协议;时间相关;谓词模态逻辑;形式化语义

中图法分类号: TP309 **文献标识码**: A

* 基金项目: 国家自然科学基金(60873260, 60903210); 国家高技术研究发展计划(863)(2009AA01Z414); 国家重点基础研究发展计划(973)(2007CB311202); 江苏省自然科学基金(BK2008090)

收稿时间: 2008-06-23; 修改时间: 2009-03-30; 定稿时间: 2009-07-06

在密码协议中,时间是影响其安全性的一个重要因素.一方面,任何协议都是对符合一定时序关系的行为序列的规定;另一方面,一些协议本身对时间关系有着严格的规定.如从保密性来说,要求消息在特定时间之前保密[1,2];从认证性来说,主体的信任状态是随时间的推移而变化的[3];从不可否认性来说,缺乏时限性可能导致公平性无法真正满足[4].因此,在分析密码协议的安全属性时,有必要将时间纳入考虑.

为了分析密码协议,人们提出了各种方法.1989 年,Burrows 等人提出的 BAN 逻辑[5]是分析安全协议的一个里程碑,它将逻辑的方法引入了安全协议验证中,极大地激发了一大批研究者投入到安全协议的形式化分析中.然而随着研究的深入,人们发现 BAN 逻辑还存在一些不足,如语义不清晰,理想化过程受人为因素影响较大;另外,BAN 逻辑注重对协议认证性的分析,但对保密性的分析能力有限[6].鉴于此,人们对 BAN 逻辑进行了各种改进,形成 BAN 类逻辑[7−9].其中,Abadi 等人提出的 AT 逻辑[8]和 Paul 等人提出的 SVO 逻辑[9]给出了逻辑语义,使得逻辑的可靠性可以得到验证,也减少了逻辑的二义性.但其逻辑语言本身未包含时间因素,只是在语义模型中使用了时间.语义中使用了时间对逻辑进行解释这一点,说明了时间在密码协议中几乎是一个不可回避的因素.语言的语法中未出现时间表明它还是无法直接描述协议中的时间特性.另外,在这些语义模型中均利用了 Kripke 语义对认知逻辑进行了解释,即定义各种可能世界间的可达关系,并基于这种可达关系对认知算子做出解释.但由于所构造的可达关系只依赖于特定的主体,而与时间无关,其实质是在一个相对固定的时间点讨论可达关系,从而没有反映出基于时间的动态特性.Coffey 等人提出一种 CS 逻辑[10],与以上 BAN 类逻辑不同的是,它将时间因素引入了逻辑中,体现出了时间在协议中的重要性.然而,CS 逻辑只针对公钥密码协议,主要用于分析一般密码协议,分析的协议范围有限,使其对安全属性的分析受限.另外,CS 逻辑也缺乏形式化语义,无法保证该逻辑的可靠性.文献[11]对 CS 逻辑进行了改进,但只是针对在分析特定协议时的改进,缺乏系统性.由于其语义不明确,导致逻辑的一致性难以保证.文献[12]针对文献[10,11]存在的问题作了进一步改进,但同样因为形式化语义的缺乏,未能完全避免其存在的问题.Zhang 等人针对密码协议中的动态信仰提出一种分析密码协议的逻辑[3],并给出形式化语义,其动态性的反映不是直接建立在时间概念上,而是建立在情景(situation)上.在其所给出的逻辑语义中,可能世界之间的可达关系未明确定义.文献[13,14]采用时序逻辑与认知逻辑相结合的方法研究协议中主体的动态信仰,即同时使用了时序算子与认知模态算子.这类方法可在一定程度上反映主体信仰的变化,但时序算子对时间的反映是隐式的、相对的、概略的,对时间特性的表达力弱于使用谓词模态逻辑,如无法反映某特定时间的安全属性.其他方法中也有将时间引入密码协议分析中的,如文献[15]在 Spi 演算中加入时间因素对密码协议进行验证,但与本文的意图有所不同,它主要针对密码的破解而言.最近两年,有关时间相关协议的研究有逐渐增加的趋势[16−18],体现了人们对时间相关密码协议的重视.

国内在时间相关密码协议逻辑方面的研究不多.2002 年,梁坚等人通过对可证明性逻辑的扩展,引入基本的时态公式“x At t”及“timestamp”对密码协议的时限责任进行了分析[19].随后,范红、冯登国基于 CS 逻辑提出了一种分析 Timed-release 公钥协议的扩展逻辑[20].赵华伟等人针对文献[20]做了进一步的改进[21],其主要目的是将 CS 逻辑扩展到对称密码系统中,并对 NS 协议进行了分析,但未体现对时间相关安全属性的分析.以上研究均未对协议分析逻辑提出严格的逻辑语义.黎波涛、罗军舟针对 Zhou-Gollmann 协议[22]及其存在的时限性问题[4]对 SVO 逻辑进行了扩展[23],并据此分析了其公平性方面的缺陷,拓宽了协议的使用范围.但其扩展是专门针对分析不可否认协议的时限性需要而提出来的,它只考虑到了对信息发送与接收行为的描述,而对逻辑中的其他公式的时间没有进行描述[23].同时,由于 SVO 逻辑语义中可达关系的定义基于固定的时间点,因此,用扩展 SVO 的方法无法真正反映认知状态的动态变化.

本文的研究基于以下几方面的考虑:

(1) 在密码协议的分析中,显式引入时间因素,使其可以分析时间相关的保密性以及与认证性相关的主体信仰的动态性.

(2) 扩展密码协议逻辑的分析范畴.包括对对称和非对称密码协议(特别是时间相关密码协议)的支持.

(3) 进一步形式化密码协议逻辑的语法,减少逻辑符号使用的随意性,为协议验证提供精确的数学描述[24].

(4) 给出协议逻辑基于可能世界的形式化语义,其中,改变目前协议逻辑中对可能世界的定义,使其能够真正地代表整个协议运行过程的全局(目前,协议逻辑中的可能世界只能看成特定于某时间点的可能世界),可能世界间的可达关系不仅特定于主体,而且特定于时间.

(5) 严格定义消息的析出与构造,以反映主体对消息的隐式处理能力.区分一个消息所包含的消息与主体可从一消息中获取的消息,使得逻辑系统对消息的表达更为合理.

(6) 在形式化语义模型的基础上研究逻辑公理,确保逻辑的可靠性.

从以上考虑出发,本文基于多类型变量的谓词模态逻辑提出一种时间相关密码协议逻辑(time-dependent cryptographic protocol logic,简称 TCPL),给出其形式化语义及可靠性证明,并分析了协议实例.

1 TCPL 的定义

1.1 语法部分

定义 1. TCPL 的形式语言(记为 L^{TCPL})由以下符号组成.

(1) 常元:A 型常元 e;T 型常元 τ_0.

(2) 变元:T 型变元:$\tau,\tau',\tau'',\ldots$;A 型变元:$i,j,\ldots,i',j',\ldots$;K 型变元:$k,k',k'',\ldots$;M 型变元:$m,m',m'',\ldots$.

(3) 函词:一元$\langle A,K\rangle$型函词 *AgentPublic*,*AgentPrivate*;一元$\langle T,K\rangle$型函词 *TimePublic*,*TimePrivate*;一元$\langle K,K\rangle$型函词 *Reverse*;二元$\langle T,T,T\rangle$型函词 *Plus*;二元$\langle A,A,K\rangle$型函词 *SharedKey*;二元$\langle M,M,M\rangle$型函词 *Combine*;二元$\langle M,K,M\rangle$型函词 *EnOrDec*.

(4) 谓词:一元$\langle M\rangle$型谓词#,二元$\langle T,T\rangle$型谓词$\leqslant$;二元$\langle M,M\rangle$型谓词 C;三元$\langle A,T,M\rangle$型谓词 R,S,H;四元$\langle A,T,M, M\rangle$型谓词 G.

(5) 等词:$\langle T,T\rangle$型等词$=_\tau$;$\langle A,A\rangle$型等词$=_a$;$\langle K,K\rangle$型等词$=_k$;$\langle M,M\rangle$型等词$=_m$.

(6) 量词:$\forall_\tau,\forall_a,\forall_k,\forall_m$.

(7) 连接词:$\neg,\rightarrow$.

(8) 模态词:$B_{i,\tau}$.

(9) 标点符号:,,(,)(逗号与括号).

定义 2. 函词缩写.

- $k_i^+ =_{def} AgentPublic(i)$.
- $k_i^- =_{def} AgentPrivate(i)$.
- $k_{\tau+}=_{def}TimePublic(\tau)$.
- $k_{\tau-}=_{def}TimePrivate(\tau)$.
- $k_{ij}=_{def}SharedKey(i,j)$.
- $[m_1,m_2]=_{def}Combine(m_1,m_2)$.
- $[m]_k=_{def}EnOrDec(m,k)$.
- $\tilde{k} =_{def} Reverse(k)$.
- $\tau+\tau'=_{def}Plus(\tau,\tau')$.

定义 3. L^{TCPL} 的项分为 T 型项、A 型项、K 型项和 M 型项,分别用 Backus Naur 范式定义.

(1) T 型项:$t_\tau::=\tau_0|\tau|t_\tau+t_\tau$.

(2) A 型项:$t_a::=i|e$.

(3) K 型项: $t_k ::= k \mid k_{t_a}^+ \mid k_{t_a}^- \mid k_{t_\tau+} \mid k_{t_\tau-} \mid k_{t_a t_a} \mid \tilde{t_k}$.

(4) M 型项: $t_m ::= m \mid t_\tau \mid t_a \mid t_k \mid [t_m,t_m] \mid [t_m]_{t_k}$.

定义 4. L^{TCPL} 的公式分为原子公式φ_A和公式φ,分别用 Backus Naur 范式定义.

- $\varphi_A::=(t_\tau\leqslant t_\tau)|C(t_m,t_m)|G(t_a,t_\tau,t_m,t_m)|R(t_a,t_\tau,t_m)|S(t_a,t_\tau,t_m)|H(t_a,t_\tau,t_m)|\#(t_m)|(t_a=_a t_a)|(t_\tau=_\tau t_\tau)|(t_k=_k t_k)|(t_m=_m t_m)$.

- $\varphi::=\varphi_A|(\neg\varphi)|(\varphi\rightarrow\varphi)|\forall_\tau\tau\varphi|\forall_a i\varphi|\forall_k k\varphi|\forall_m m\varphi|B_{i,\tau}\varphi$.

定义 5. 设φ,ψ为公式,定义连接词缩写.

- $(\varphi\vee\psi)=_{def}((\neg\varphi)\rightarrow\psi)$.
- $(\varphi\wedge\psi)=_{def}(\neg(\varphi\rightarrow(\neg\psi)))$.
- $(\varphi\leftrightarrow\psi)=_{def}((\varphi\rightarrow\psi)\wedge(\psi\rightarrow\varphi))$.

定义 6. 等词缩写.

- $(\tau\neq_\tau\tau')=_{def}(\neg(\tau=_\tau\tau'))$.
- $(k\neq_k k')=_{def}(\neg(k=_k k'))$.
- $(i\neq_a j)=_{def}(\neg(i=_a j))$.
- $(m\neq_m m')=_{def}(\neg(m=_m m'))$.

定义 7. 谓词缩写.

- $(\tau<\tau')=_{def}((\tau\leqslant\tau')\wedge(\tau\neq_\tau\tau'))$.
- $(\tau>\tau')=_{def}(\neg(\tau\leqslant\tau'))$.
- $(\tau\geqslant\tau')=_{def}((\tau>\tau')\vee(\tau=_\tau\tau'))$.
- $(\tau_1*\tau_2*\ldots*\tau_n)=_{def}((\tau_1*\tau_2)\wedge(\tau_2*\tau_3)\wedge\ldots\wedge(\tau_{n-1}*\tau_n))$(其中,$*\in\{<,>,\leqslant,\geqslant,=_\tau\}$).
- $O(m)=_{def}\forall_m m_1\forall_m m_2\forall_m m_3(m\neq_m[m_1]_k\wedge m\neq_m[m_2,m_3])$.
- $H!(i,\tau,m)=_{def}H(i,\tau,m)\wedge\forall_a j(j\neq_a i\rightarrow\neg H(j,\tau,m))$.

定义 8. 量词缩写.

- $\exists_\tau\tau\varphi=_{def}\neg\forall_\tau\tau\neg\varphi$.
- $\exists_a i\varphi=_{def}\neg\forall_a i\neg\varphi$.
- $\exists_k k\varphi=_{def}\neg\forall_k k\neg\varphi$.
- $\exists_m m\varphi=_{def}\neg\forall_m m\neg\varphi$.

约定 1. 优先级(括号省略原则).

(1) 公式最外面的括号可以省略.

(2) 公式所含的联结符的优先级由高到低排列如下:$\neg,=,\wedge,\vee,\rightarrow,\leftrightarrow$(其中,=包括$=_\tau,=_a,=_k,=_m$).

(3) $B_{i,\tau}$的优先级与$\neg$相同.

(4) 同类联结词满足右向结合律.

1.2 公理系统

TCPL 的公理系统由公理模式和推理规则及其全称化组成.

A1. 所有多型变元谓词逻辑的公理模式(含等词)以及算术系统的公理.

A2. 巴肯(Barcan)公式.

(a) $\forall xB_{i,\tau}\varphi\leftrightarrow B_{i,\tau}\forall x\varphi$.

(b) $\exists xB_{i,\tau}\varphi\leftrightarrow B_{i,\tau}\exists x\varphi$.

其中,x 为任一类型的变量,$\forall,\exists$为与 x 的型相应的量词,并且当 x 为 A 型变量或 T 型变量时,要求 x 不在模态词 $B_{i,\tau}$中出现.

A3. 单调性公理.

(a) $H(i,\tau,m)\rightarrow\forall_\tau\tau'((\tau'\geqslant\tau)\rightarrow H(i,\tau',m))$.

(b) $B_{i,\tau}\varphi\rightarrow\forall_\tau\tau'((\tau'\geqslant\tau)\rightarrow B_{i,\tau'}\varphi)$.

在有时限性要求的协议中,以上公理仅在协议所给定的时间限制内成立.

A4. 时间公理.

(a) $\tau\leqslant\tau$,

(b) $\tau\leqslant\tau'\wedge\tau'\leqslant\tau''\rightarrow\tau\leqslant\tau''$.

A5. 密钥公理.

(a) $\tau \prec \tau' \wedge j \neq_a i \wedge H(i,\tau,k_{\tau'-}) \rightarrow \neg H(j,\tau,k_{\tau'-})$.

(b) $H(i,\tau,k_i^-) \wedge (j \neq_a i \rightarrow \neg H(j,\tau,k_i^-))$.

(c) $H(i,\tau,k_{ij}) \wedge H(j,\tau,k_{ij}) \wedge ((i' \neq_a i) \wedge (i' \neq_a j) \rightarrow \neg H(i',\tau,k_{ij}))$.

(d) $(\widetilde{k_i^+} =_k k_i^-) \wedge (\widetilde{k_i^-} =_k k_i^+)$;

(e) $(\widetilde{k_{\tau+}} =_\tau k_{\tau-}) \wedge (\widetilde{k_{\tau-}} =_\tau k_{\tau+})$;

(f) $\widetilde{k_{ij}} =_a k_{ij}$.

A6. 获取公理.

(a) $G(i,\tau,m,m)$.

(b) $H(i,\tau,\tilde{k}) \rightarrow G(i,\tau,[m]_k,m)$.

(c) $G(i,\tau,[m,m'],m) \wedge G(i,\tau,[m,m'],m')$.

(d) $G(i,\tau,m,m') \wedge G(i,\tau,m',m'') \rightarrow G(i,\tau,m,m'')$.

A7. 包含公理.

(a) $\exists_a i \exists_\tau \tau G(i,\tau,m,m') \rightarrow C(m,m')$.

(b) $C(m,m') \wedge C(m',m'') \rightarrow C(m,m'')$.

A8. 主体行为公理.

(a) $R(i,\tau,m) \wedge C(m,m') \rightarrow \exists_a j \exists_\tau \tau' \exists_m m''((\tau' < \tau) \wedge C(m'',m') \wedge S(j,\tau',m'') \wedge H(j,\tau',m'))$.

(b) $R(i,\tau,m) \wedge C(m,[m']_{k_j^-}) \wedge C([m']_{k_j^-},m') \rightarrow \exists_\tau \tau \exists_m m''((\tau' < \tau) \wedge C(m'',m') \wedge S(j,\tau',m'') \wedge H(j,\tau',m'))$.

(c) $R(i',\tau,m) \wedge C(m,[m']_{k_{ij}}) \wedge C([m']_{k_{ij}},m') \rightarrow$

$\exists_\tau \tau \exists_m m''((\tau' < \tau) \wedge C(m'',m') \wedge (S(i,\tau',m'') \wedge H(i,\tau',m') \vee (S(j,\tau',m'') \wedge H(j,\tau',m')))$.

(d) $O(m) \wedge (j \neq_a i) \wedge H!(j,\tau,m) \wedge H(j,\tau',m) \rightarrow$

$\exists_m m' \exists_\tau \tau''((\tau \prec \tau'' \leqslant \tau') \wedge R(j,\tau'',m') \wedge G(j,\tau'',m',m)) \wedge \exists_m m' \exists_\tau \tau''((\tau \prec \tau'' \leqslant \tau') \wedge S(j,\tau'',m') \wedge C(m',m))$.

(e) $\neg H(i,\tau,k) \wedge H(i,\tau,[m]_k) \rightarrow \exists_\tau \tau' \exists_m m'((\tau' < \tau) \wedge R(i,\tau',m') \wedge G(i,\tau,m',[m]_k))$.

A9. 拥有公理.

(a) $R(i,\tau,m) \rightarrow H(i,\tau,m)$.

(b) $S(i,\tau,m) \rightarrow H(i,\tau,m)$.

(c) $H(i,\tau,m) \wedge G(i,\tau,m,m') \rightarrow H(i,\tau,m')$.

(d) $H(i,\tau,m) \wedge H(i,\tau,m') \rightarrow H(i,\tau,[m,m'])$.

(e) $H(i,\tau,m) \wedge H(i,\tau,k) \rightarrow H(i,\tau,[m]_k)$.

A10. 新鲜性公理.

(a) $\#(m) \wedge S(i,\tau,m) \rightarrow (\tau_0 \leqslant \tau)$.

(b) $C(m,m') \wedge \#(m') \rightarrow \#(m)$.

A11. 信任公理.

(a) $B_{i,\tau}(\varphi \rightarrow \psi) \wedge B_{i,\tau}\varphi \rightarrow B_{i,\tau}\psi$.

(b) $S(i,\tau,m) \rightarrow B_{i,\tau}S(i,\tau,m)$.

(c) $R(i,\tau,m) \rightarrow B_{i,\tau}R(i,\tau,m)$.

(d) $H(i,\tau,m) \rightarrow B_{i,\tau}H(i,\tau,m)$.

IR. 推理规则(inference rule).

(a) $\dfrac{\varphi \rightarrow \psi, \varphi}{\psi}$.

(b) $\dfrac{\vdash \varphi}{\vdash B_{i,\tau}\varphi}$.

2 TCPL 的语义

2.1 TCPL的模型

直观上说,协议就是由一组主体按照规定的行为序列及消息格式进行信息交流的过程.协议的参与者组成协议的主体集合 $\boldsymbol{A}$.每个主体有其初始状态,我们用 $q_i^{\tau_0}$ 表示主体 i 的初始状态,它反映了主体 i 在协议执行之前所拥有消息,它是一个静态的概念.在一个给定时间,每个主体都有其行为历史,行为历史常用主体自协议开始执行以来的行为序列 σ_i^{τ} 表示.我们用初始状态和行为历史来定义可能世界,并通过定义可能世界间的可达关系对模态词进行解释.以下给出详细定义.

定义 9. TCPL 的论域 $D=A\cup T\cup K\cup M$,其中:

(1) $\boldsymbol{A}$ 为主体集合,即密码协议的所有参与者或可能的参与者.

(2) $\boldsymbol{T}$ 为时间集合,为整数的有限子集.$\leqslant$为 $\boldsymbol{T}$ 上的小于等于关系,τ_0 表示 0,为协议运行的起始时间.这里,我们用离散时间对协议中的时间因素进行建模.

(3) $\boldsymbol{K}$ 为密钥集合.密钥分为主体相关公钥及私钥、时间相关公钥及私钥、共享密钥以及其他一些密钥(如临时会话密钥)等.主体相关私钥在任何时候只能由其所相关的主体拥有,时间相关私钥在其所相关的时间之前只能由其生成者拥有.共享密钥在任何时候只能由共享该密钥的主体拥有.如果用一个密钥加密的消息可用另一密钥解密,则称这两个密钥互逆,记密钥 k 的逆为 $\tilde{k}$.规定主体相关的公钥与同一主体相关的私钥互逆,时间相关的公钥与同一时间相关的私钥互逆,共享密钥与其自身互逆.

(4) $\boldsymbol{M}$ 为消息集合,包括原子消息、加密消息和组合消息.其中,原子消息包括主体、时间、密钥、随机数及单个明文消息等未经组合或加密的消息.设任意 $m\in M,k\in K$,则加密消息为利用 k 对 m 加密后形成的消息,记为$[m]_k$.设任意 $m\in M,m'\in M$,则组合消息为 m 和 m'的并置,记为$[m,m']$.

定义 10. 给定消息 m,称 $contain(m)$为 m 中所包含的消息的集合.形式化地,递归定义 $contain(m)$如下:

(1) $m\in contain(m)$.

(2) 如果$[m',m'']\in contain_K(m)$,则 $m'\in contain(m)$且 $m''\in contain(m)$.

(3) 如果$[m']_k\in contain_K(m)$,则 $m'\in contain(m)$.

定义 11. 给定密钥集合 K 及消息集合 M,称 $extract_K(M)$为利用 K 中的密钥可从 M 中析出的消息集合.形式化地,递归定义 $extract_K(M)$如下:

(1) 如果 $m\in M$,则 $m\in extract_K(M)$.

(2) 如果$[m,m']\in extract_K(M)$,则 $m\in extract_K(M)$且 $m'\in extract_K(M)$.

(3) 如果$[m]_k\in extract_K(M)$,且有 $\tilde{k}\in K$ 或 $\tilde{k}\in extract_K(M)$,则 $m\in extract_K(M)$.

当 M 只包含单个消息 m 时,$extract_K(M)$为 $extract_K(\{m\})$,简记为 $extract_K(m)$.

定义 12. 给定密钥集合 K 及消息集合 M,称 $construct_K(M)$为利用 K 中的密钥和 M 中的消息可构造出的消息集合.形式化地,递归定义 $construct_K(M)$如下:

(1) 如果 $m\in M$,则 $m\in construct_K(m)$.

(2) 如果$[m,m']\in construct_K(M)$,则 $m\in construct_K(M)$且 $m'\in construct_K(M)$.

(3) 如果$[m]_k\in construct_K(M)$,且有 $\tilde{k}\in K$ 或 $\tilde{k}\in extract_K(M)$,则 $m\in construct_K(M)$.

(4) 如果 $m\in construct_K(M),m'\in construct_K(M)$,则$[m,m']\in construct_K(M)$.

(5) 如果 $m\in construct_K(M)$,且有 $k\in K$ 或 $k\in extract_K(M)$,则$[m]_k\in construct_K(M)$.

当 M 只包含单个消息 m 时,$construct_K(M)$为 $construct_K(\{m\})$,简记为 $construct_K(m)$.

定义 13. 协议状态机是一个四元组(Q,E,δ,q_0),其中:

(1) Q 为主体状态集.主体 i 在 τ 时刻的状态为 $q_i^\tau=(M_i^\tau,K_i^\tau)$,其中: M_i^τ 为 i 在 τ 时所生成的或收到的原始消息集合,即主体 i 未对其进行过析出或构造; K_i^τ 为主体 i 在 τ 时所拥有的密钥集合.特别地,q_0 为协议的初始状态,初始状态可看作是由主体在 τ_0 之前生成或收到的消息集合及密钥集合组成.

(2) E 为主体行为集合.一个主体在协议中可执行的行为有 3 种:发送消息(*send*(*m*))、接收消息(*receive*(*m*))以及生成消息(*generate*(*m*)).规定,主体可同时执行多种行为.用 $e,e_1,e_2,\ldots$ 表示单个行为,用 α_i^τ 表示主体 i 在 τ 时的行为集合,则 $e\in\{send(m),receive(m),generate(m)\}$, $\alpha_i^\tau\subseteq\{send(m),receive(m),generate(m)\}$.主体在协议中的所有行为按照时间先后顺序的排列形成主体的行为序列.

对于生成消息有如下限制:(i) 主体只能生成原子消息;(ii) 任何时候某主体生成了一个消息,则其他任何主体在任何时候都不能生成该消息;(iii) 在一个消息被生成之前,任何人都不拥有该消息.

发送消息可分为首次发送和转发,其形式化定义在定义 15 中给出.

(3) $\delta: Q\times 2^E\to Q$ 为状态转换函数,表示主体 i 的行为对其状态的改变.具体来说,设 $q_i^\tau=(M_i^\tau,K_i^\tau)$ 且 i 的下一行为的发生时间为 $\tau'(\tau<\tau')$,则

$$q_i^{\tau'}=(M_i^{\tau'},K_i^{\tau'})=\delta(q_i^\tau,\alpha_i^{\tau'})=\begin{cases}(M_i^\tau,K_i^\tau), & 当\alpha_i^{\tau'}=\{send(m)\}\\ (M_i^\tau\cup\{m\},K_i^\tau\cup key(extract_{K_i^\tau}(m))), & 当\alpha_i^{\tau'}=\{receive(m)\}\\ (M_i^\tau\cup\{m\},K_i^\tau\cup key(\{m\})), & 当\alpha_i^{\tau'}=\{generate(m)\}\end{cases},$$

其中,*key* 为密钥选择函数.给定一个消息集合 M,如果 $k\in M$ 且 $k\in K$,则 $k\in key(M)$.由于协议本身规定了消息的格式,因此,协议的参与者有足够的能力做出这种选择.

由上式可见,发送消息对主体的状态并无影响.而协议均是从单个发送消息的行为开始的,即主体在 τ_0 时的行为并未改变其初始状态.因此,下文直接用 $q_i^{\tau_0}=(M_i^{\tau_0},K_i^{\tau_0})$ 表示主体 i 的初始状态.

当主体 i 在 τ 时的行为不止一个时,设 $\alpha_i^\tau=\{e_1,e_2,\ldots,e_n\}$,则 $\delta(q_i^\tau,\alpha_i^{\tau'})=\bigcup_{e\in\alpha_i^{\tau'}}\delta(q_i^\tau,\{e\})$.其中,将状态的并定义如下:设 $q'=(M',K'),q''=(M'',K'')$,则 $q'\cup q''=(M'\cup M'',K'\cup K'')$.

定义 13 中所涉及的状态,实际上可以看作主体在协议中的局部状态.由定义可见,主体局部状态的改变是由其一定的行为引起的,但从状态本身无法知道该状态是如何形成的.另外,某一行为的执行并不必然导致状态的改变(如发送消息).因此,为了更加全面地反映协议,在考虑状态因素的同时必须考虑其行为历史.

定义 14. Σ为行为历史集合,表示主体自协议执行以来的行为序列.一般地,用 $\sigma_i^\tau=\alpha_i^{\tau_0}\alpha_i^{\tau_1}\ldots\alpha_i^\tau$ 表示主体 i 在 τ 时的行为历史.扩展定义 13 中的状态转换函数为 $\bar{\delta}: Q\times\Sigma\to Q$,则对主体 i 在 τ 时的状态 q_i^τ ,有

$$q_i^\tau=\bar{\delta}(q_i^{\tau_0},\sigma_i^\tau)=\delta(\ldots\delta(\delta(q_i^{\tau_0},\alpha_i^{\tau_1}),\alpha_i^{\tau_2}),\ldots,\alpha_i^\tau).$$

有了行为历史的概念,我们可以形式化地定义消息的首次发送和转发的概念.

定义 15. 称主体 i 在 τ 时通过 m' 首次发送了消息 m(简称主体 i 在 τ 时首发了消息 m),是指 $m\in contain(m')$, $send(m')\in\sigma_i^\tau$ 且不存在 i',τ',m'',使得 $i'\neq i,\tau'<\tau,m\in contain(m'')$且 $send(m'')\in\sigma_{i'}^{\tau'}$.否则,称主体 i 在 τ 时通过 m' 转发了消息 m.

定义 16. 主体 i 在 τ 时的局部世界 $\omega_i^\tau=(q_i^{\tau_0},\sigma_i^\tau)$,其中, $q_i^{\tau_0}$ 表示主体 i 的初始状态, σ_i^τ 表示主体 i 在 τ 时的行为历史.

在此,我们区分了局部世界和局部状态.通过局部世界(包括初始状态和行为历史),使用状态转换函数可以很方便地得到主体的各种局部状态,但反之却不行.可见,局部世界的概念与局部状态的概念相比,能更为充分地描述协议,它体现了静态状态与动态行为的结合.

定义 17. 特定于时间 τ 的局部世界由所有主体在 τ 时的局部世界组成,以向量方式记为 $\omega^\tau=(\omega_i^\tau,\omega_j^\tau,\ldots,\omega_e^\tau)$;特定于主体 i 的局部世界由主体 i 在所有时间的局部世界组成,以向量方式记为 $\omega_i=(\omega_i^{\tau_0},\omega_i^{\tau_1},\ldots,\omega_i^{\tau_n})^T$.

定义 18. 协议的全局世界由所有局部世界组成,用矩阵表示为

$$\omega=\begin{pmatrix}\omega_i^{\tau_0} & \omega_j^{\tau_0} & \dots & \omega_e^{\tau_0}\\ \omega_i^{\tau_1} & \omega_j^{\tau_1} & \dots & \omega_e^{\tau_1}\\ \vdots & \vdots & \vdots & \vdots\\ \omega_i^{\tau_n} & \omega_j^{\tau_n} & \dots & \omega_e^{\tau_n}\end{pmatrix}=(\omega_i \quad \omega_j \quad \dots \quad \omega_e)=\begin{pmatrix}\omega^{\tau_0}\\ \omega^{\tau_1}\\ \vdots\\ \omega^{\tau_n}\end{pmatrix}.$$

W 为协议的所有可能的全局世界的集合,简称可能世界.下文中,$\omega_i^\tau, q_i^\tau(\omega)$ 分别表示在可能世界ω中,主体 i 在τ时的局部世界及局部状态;用 $\alpha_i^\tau(\omega), \sigma_i^\tau(\omega)$ 分别表示在可能世界ω中,主体 i 在τ时的行为及行为历史;用 $M_i^\tau(\omega), K_i^\tau(\omega)$ 分别表示在可能世界ω中,主体 i 在τ时所拥有的原始消息集合及密钥集合.

任一$\omega\in W$ 应满足如下条件:

(1) 存在主体收到某消息,则一定存在主体在此之前发送过该消息.即,如果有 $receive(m)\in\alpha_i^\tau(\omega)$ 则一定存在$\tau'<\tau, j\in A$,使得 $send(m)\in\alpha_j^{\tau'}(\omega)$.特别地,存在主体收到包含消息 m 的消息,则一定存在主体在此之前通过某消息首发了消息 m;

(2) 主体只能发送自己拥有的信息.即,如果存在 i,τ使得 $send(m)\in\alpha_i^\tau(\omega)$,则一定有

$$m\in construct_{K_i^\tau(\omega)}(M_i^\tau(\omega)).$$

特别地,如果主体通过某消息首发了消息 m,则该主体一定拥有消息 m.

定义 19(行为历史的相等). 设 $\sigma_i^\tau(\omega_1)=\alpha_i^{\tau_0}(\omega_1)\alpha_i^{\tau_1}(\omega_1)...\alpha_i^\tau(\omega_1), \sigma_i^\tau(\omega_2)=\alpha_i^{\tau_0}(\omega_2)\alpha_i^{\tau_1}(\omega_2)...\alpha_i^\tau(\omega_2)$,称 $\sigma_i^\tau(\omega_1)=\sigma_i^\tau(\omega_2)$,当且仅当对任意的$\tau', \tau_0\leqslant\tau'\leqslant\tau$有 $\alpha_i^{\tau'}(\omega_1)=\alpha_i^{\tau'}(\omega_2)$.

定义 20(可达关系). 可能世界间的可达关系被定义为 $R_i^\tau\subseteq W\times W$.设$\omega,\omega'\in W$,称 $\omega R_i^\tau\omega'$ 当且仅当 $\omega_i^\tau=\omega_i'^\tau$.

定义 21. TCPL 的模型 $\mathfrak{M}=(W,(R_i^\tau)_{(i\in A,\tau\in T)},D,I)$ 由以下 4 部分组成:

(1) 集合 $\boldsymbol{W}$,具体见定义 18,其元素为可能世界,常用$\omega,\omega',\omega_1,\omega_2,\dots$表示.

(2) 集合 $\boldsymbol{D}$,具体见定义 9.约定对于同一协议来说,$\boldsymbol{D}$ 为各可能世界的公用论域.

(3) $R_i^\tau\subseteq W\times W$ 为可能世界间的可达关系,具体见定义 20.与一般模态逻辑不同的是,R_i^τ 并非单个关系,而是一个关系的集合,对于任意 $i\in A,\tau\in T$ 均有一个相应的可达关系 R_i^τ.

(4) I 为一解释,它指称 L^{TCPL} 中的常元、函词、谓词、等词和模态词.

对任一常元 c,$I(c)$为与 c 相应的论域中的一个元素,简记为 $\overline{c}$.

对每一函词 $f^{(n)}$,$I(f^{(n)})$为与 $f^{(n)}$的型相应的论域上的 n 元函数,记为 $\overline{f}^{(n)}$.

对每一谓词 $P^{(n)}$,$I(P^{(n)})$为与 $P^{(n)}$的型相应的论域上的 n 元关系,记为 $\overline{P}^{(n)}$ (将等词和模态词看作特殊的谓词).

为描述方便,在不产生混淆的情况下,我们在模型内将一些语法符号解释给其自身.例如,如果 c 为常元,f 为函词,则 $I(c)=c, I(f)=f$,下文将给出其具体含义.该约定仅仅是从符号表示的方便考虑的,根据上下文,不难判定其是语法表示还是语义表示.

2.2 TCPL的基本语义

TCPL 的语义包括对变元取值的指派、对项的指称、对公式真值条件的规定.我们在 TCPL 的模型中对其进行讨论,并由以下定义给出:

定义 22. 指派是指映射 $s:\{v_1,v_2,v_3,\dots\}\to D$,其中,$v_i$ 表示变量(包括各型变量).即,对任一 $i=1,2,3\dots, s(v_i)\in D$.即,$s$ 对各型变元指派其相应论域中的个体作为其取值.为表述方便,未对 D 中各子论域进行区分,但应该明确,某一型的变量只能被映射到 D 中与该型变量相应的子论域中(下文默认这一约定).

定义 23. 项的指称是指从项到论域 D 的映射,可通过对 s 的扩展得来[25].定义 $\overline{s}$ 为项集合到论域的映射,对任意项 t,有

$$\overline{s}(t)=\begin{cases}s(v), & \text{当}t\text{为变元}v\text{时}\\ \overline{c}, & \text{当}t\text{为常元}c\text{时}\\ \overline{f}^{(n)}(\overline{s}(t_1),\dots,\overline{s}(t_n)), & \text{当}t\text{为}n\text{元函数}f^{(n)}(t_1,\dots,t_n)\text{时}\end{cases}.$$

定义 24. 解释 I 的具体定义如下(本定义中谓词的表示式指谓词命名式):

- $I(e)$为攻击者,它抽象了所有可能的攻击者以及各种环境因素.
- $I(\tau_0)$为协议执行的起始时间.
- $I(AgentPublic(i))$,即 $I(k_i^+)$,表示主体 $\overline{s}(i)$ 的公钥.
- $I(AgentPrivate(i))$,即 $I(k_i^-)$,表示主体 $\overline{s}(i)$ 的私钥.
- $I(TimePublic(i))$,即 $I(k_{\tau+})$表示与时间 $\overline{s}(\tau)$ 相关联的公钥,称为时间 $\overline{s}(\tau)$ 的公钥.
- $I(TimePrivate(i))$,即 $I(k_{\tau-})$表示与时间 $\overline{s}(\tau)$ 相关联的私钥,称为时间 $\overline{s}(\tau)$ 的私钥.
- $I(SharedKey(i,j))$,即 $I(k_{ij})$,表示主体 $\overline{s}(i)$ 和 $\overline{s}(j)$ 的共享密钥.
- $I(Combine(m_1,m_2))$,即 $I([m_1,m_2])$,表示消息 $\overline{s}(m_1)$ 与 $\overline{s}(m_2)$ 的组合消息.
- $I(EnOrDed(m,k))$,即 $I([m]_k)$,表示用密钥 $\overline{s}(k_1)$ 对消息 $\overline{s}(m)$ 进行的加密或解密.
- $I(Reverse(k))$,即 $I(\tilde{k})$,表示密钥 $\overline{s}(k)$ 的逆,表示为 $\widetilde{\overline{s}(k)}$.
- $I(Plus(\tau,\tau'))$,即 $I(\tau+\tau')$,表示时间 $\overline{s}(\tau)$ 与 $\overline{s}(\tau')$ 之和.
- $I(C(m,m'))$表示消息 $\overline{s}(m)$ 包含消息 $\overline{s}(m')$.
- $I(\tau_1 \leqslant \tau_2)$表示时间 τ_1 先于时间 τ_2,即 $\overline{s}(\tau_1) \leqslant \overline{s}(\tau_2)$.此处为表述的方便,直接将$\leqslant$解释为 T 上的$\leqslant$关系;
- $I(S(i,\tau,m))$表示主体 $\overline{s}(i)$ 在时间 $\overline{s}(\tau)$ 时发送消息 $\overline{s}(m)$.
- $I(R(i,\tau,m))$表示主体 $\overline{s}(i)$ 在时间 $\overline{s}(\tau)$ 时接收消息 $\overline{s}(m)$.
- $I(H(i,\tau,m))$表示主体 $\overline{s}(i)$ 在时间 $\overline{s}(\tau)$ 时拥有消息 $\overline{s}(m)$.
- $I(\#(m))$表示消息 $\overline{s}(m)$ 是新鲜的.
- $I(G(i,\tau,m,m'))$表示在时间 $\overline{s}(\tau)$ 时,主体 $\overline{s}(i)$ 可从消息 $\overline{s}(m)$ 中获取消息 $\overline{s}(m')$.
- $I(i=_a j)$表示 $\overline{s}(i) =_a \overline{s}(j)$,其中,$=_a$ 表示集合 A 上的相等关系.
- $I(\tau=_\tau \tau')$表示 $\overline{s}(\tau) =_\tau \overline{s}(\tau')$,其中,$=_\tau$表示集合 T 上的相等关系.
- $I(k_1=_k k_2)$表示 $\overline{s}(k_1) =_k \overline{s}(k_2)$,其中,$=_k$ 表示集合 K 上的相等关系.
- $I(m_1=_m m_2)$表示 $\overline{s}(m_1) =_m \overline{s}(m_2)$,其中,$=_m$ 表示集合 M 上的相等关系.
- $I(B_{i,\tau}\varphi)$表示主体 $\overline{s}(i)$ 在时间 $\overline{s}(\tau)$ 相信命题 $I(\varphi)$.

根据以上解释,我们也可以给出一些缩写谓词的解释,如 $O(m)$被解释为 m 为原子消息;$H!(i,\tau,m)$被解释为主体 i 在τ时单独拥有消息 m.

定义 25(公式的真值条件). 用 $\vDash^{\omega}_{\mathfrak{M}} \varphi$ [s](简记为 $\vDash^{\omega}_{\mathfrak{M}} \varphi$)表示公式φ在模型 $\mathfrak{M}$ 的可能世界ω中对指派 s 真,“iff”表示“当且仅当”,则公式(1) $\vDash^{\omega}_{\mathfrak{M}} (t_\tau \leqslant t'_\tau)$ iff $\overline{s}(t_\tau) \leqslant \overline{s}(t'_\tau)$.

(2) $\vDash^{\omega}_{\mathfrak{M}} C(t_m,t'_m)$ iff $\overline{s}(t'_m) \in contain(\overline{s}(t_m))$.

(3) $\vDash^{\omega}_{\mathfrak{M}} G(t_a,t_\tau,t_m,t'_m)$ iff $\overline{s}(t'_m) \in extract_{K^{\overline{s}(t_\tau)}_{\overline{s}(t_a)}(\omega)}(\overline{s}(t_m))$.

(4) $\vDash^{\omega}_{\mathfrak{M}} H(t_a,t_\tau,t_m)$ iff $\overline{s}(t_m) \in construct_{K^{\overline{s}(t_\tau)}_{\overline{s}(t_a)}(\omega)}(M^{\overline{s}(t_\tau)}_{\overline{s}(t_a)}(\omega))$.

(5) $\vDash^{\omega}_{\mathfrak{M}} S(t_a,t_\tau,t_m)$ iff $send(\overline{s}(t_m)) \in \alpha^{\overline{s}(t_\tau)}_{\overline{s}(t_a)}(\omega)$.

(6) $\vDash^{\omega}_{\mathfrak{M}} R(t_a,t_\tau,t_m)$ iff $receive(\overline{s}(t_m)) \in \alpha^{\overline{s}(t_\tau)}_{\overline{s}(t_a)}(\omega)$.

(7) $\vDash^{\omega}_{\mathfrak{M}} \#(t_m)$ iff 存在 $m \in M$ 使得 $m \in contain(\overline{s}(t_m))$,且对任意 $i \in A, \tau \in T$,如果 $\tau \prec \tau_0$,则 $send(\overline{s}(m)) \notin \alpha^{\tau}_i(\omega)$.

(8) $\vDash^{\omega}_{\mathfrak{M}} (t_a =_a t'_a)$(或 $\vDash^{\omega}_{\mathfrak{M}} (t_\tau =_\tau t'_\tau), \vDash^{\omega}_{\mathfrak{M}} (t_k =_k t'_k), \vDash^{\omega}_{\mathfrak{M}} (t_m =_m t'_m)$) iff
$\overline{s}(t_a) =_a \overline{s}(t'_a)$(或$\overline{s}(t_\tau) =_\tau \overline{s}(t'_\tau), \overline{s}(t_k) =_k \overline{s}(t'_k), \overline{s}(t_m) =_m \overline{s}(t'_m)$) .

(9) $\vDash^{\omega}_{\mathfrak{M}} (\neg\varphi)$ iff $\nvDash^{\omega}_{\mathfrak{M}} \varphi$.

(10) $\vDash^{\omega}_{\mathfrak{M}} (\varphi \to \psi)$ iff $\nvDash^{\omega}_{\mathfrak{M}} \varphi$或 $\vDash^{\omega}_{\mathfrak{M}} \psi$.

(11) $\vDash^{\omega}_{\mathfrak{M}} (\forall_a i\varphi(i))$(或 $\vDash^{\omega}_{\mathfrak{M}} (\forall_\tau \tau\varphi(\tau)), \vDash^{\omega}_{\mathfrak{M}} (\forall_k k\varphi(k)), \vDash^{\omega}_{\mathfrak{M}} (\forall_m m\varphi(m))$) iff 对任意的 $\theta \in A$(或 $\iota \in T, \kappa \in K, \mu \in M$),有
$\vDash^{\omega}_{\mathfrak{M}} \varphi[\theta]$(或 $\vDash^{\omega}_{\mathfrak{M}} \varphi[\iota], \vDash^{\omega}_{\mathfrak{M}} \varphi[\kappa], \vDash^{\omega}_{\mathfrak{M}} \varphi[\mu]$),

其中,对$\varphi[\theta]$(或$\varphi[\iota],\varphi[\kappa],\varphi[\mu]$)说明如下[26]:考虑在$L^{TCPL}$中额外定义$A$型常量$c_a$(或$T$型常量$c_\tau$,$K$型常量$c_k$,$M$型常量$c_m$),形成扩展语言$L^{TCPL}\cup\{c_a\}$(或$L^{TCPL}\cup\{c_\tau\}$,$L^{TCPL}\cup\{c_k\}$,$L^{TCPL}\cup\{c_m\}$),并将其模型扩展为$\mathfrak{M}_\theta^{c_a}$(或$\mathfrak{M}_\iota^{c_\tau},\mathfrak{M}_\kappa^{c_k},\mathfrak{M}_\mu^{c_m}$),在$\mathfrak{M}_\theta^{c_a}$(或$\mathfrak{M}_\iota^{c_\tau},\mathfrak{M}_\kappa^{c_k},\mathfrak{M}_\mu^{c_m}$)中,将$c_a$(或$c_\tau,c_k,c_m$)解释为$A$(或$T,K,M$)中的$\theta$(或$\iota,\chi,\mu$),其余解释与模型$\mathfrak{M}$保持相同,则

$\models_{\mathfrak{M}}^{\omega}\varphi[\theta]$(或$\models_{\mathfrak{M}}^{\omega}\varphi[\iota],\models_{\mathfrak{M}}^{\omega}\varphi[\kappa],\models_{\mathfrak{M}}^{\omega}\varphi[\mu]$) iff $\models_{\mathfrak{M}_\theta^{c_a}}^{\omega}\varphi(c_a)$(或$\models_{\mathfrak{M}_\iota^{c_\tau}}^{\omega}\varphi(c_\tau),\models_{\mathfrak{M}_\kappa^{c_k}}^{\omega}\varphi(c_k),\models_{\mathfrak{M}_\mu^{c_m}}^{\omega}\varphi(c_m)$).

(12) $\models_{\mathfrak{M}}^{\omega}B_{i,\tau}\varphi$ iff 对所有$\omega'\in W$,如果$\omega R_{\bar{s}(i)}^{\bar{s}(\tau)}\omega'$,则有$\models_{\mathfrak{M}}^{\omega'}\varphi$.

基于 TCPL 的语义,可以证明该逻辑的可靠性(soundness).基本方法是:首先证明各公理及其全称式的有效性、推理规则的保有效性;然后,通过对证明序列长度使用归纳法来证明逻辑的可靠性.对 TCPL 可靠性的形式化描述与证明见附录.

3 协议分析

TCPL 可用于多种密码协议的分析与验证.通常密码协议的验证目标有多种,最重要的如保密性和认证性;在电子商务协议中,人们还关心不可否认性及公平性等属性.保密性表明一个主体是否拥有一消息,在 TCPL 中通常用 $H(i,\tau,m)$或$\neg H(i,\tau,m)$来表达.对前者的证明可直接证明,对后者的证明通常使用反证法.认证性表明一个主体对某一行为的信任状态,在 TCPL 中通常用模态词 $B_{i,\tau}\varphi$来表达认证性.不可否认性表明一个主体对自己的行为不可否认,通常以是否能够让仲裁者相信相关事实来表达不可否认性;也用模态词 $B_{i,\tau}\varphi$来表达,这时的 i 表示仲裁者.公平性表明协议任何一步执行后的中止将不会破坏通信双方主体的地位的公平性,即在协议中的每个时间点要么双方都拥有期望消息,要么都不拥有期望消息.可见,公平性在事实上与时间密切相关,可利用 TCPL 具有时间因素的公式组合来表达.

3.1 基于TCPL分析密码协议的一般过程

在给出协议分析一般过程之前,先给出如下几个定义.

定义 26. 协议是协议语句的序列,协议语句是对一次信息交换的描述.协议语句具有 $i\to j:m$ 或 $i\leftarrow j:m$(一般用在电子商务协议中)的形式,其中,$i\to j:m$ 表示主体 i 向主体 j 发送消息 m,$i\leftarrow j:m$ 表示主体 i 从主体 j 处主动获取消息 m.通常,用 $\hat{P}$ 表示一个协议.

定义 27. 时间关联是指按照协议所设计的执行顺序给每个协议语句分别关联上消息项被发送及接收时间的过程.关联时间后的协议语句具有$\tau_n(i\to j:m)\tau_{n+1}$或$\tau_{n+1}(j\leftarrow i:m)\tau_n$的形式,前者表示主体 i 在τ_n时发送消息 m,主体 j 在τ_{n+1}时收到消息 m;后者表示 i 在τ_n时发布消息 m,主体 j 在τ_{n+1}时获取消息 m.常用 P_t表示经过时间关联的协议.

定义 28. 协议的形式化是指将协议转换为 TCPL 中的逻辑公式的过程,并将这些逻辑公式的集合称为形式化协议,在不致引起混淆的情况下也简称协议,记为 P.

这里的协议形式化与 BAN 逻辑中协议的理想化过程相比有比较确定的模式,一般来说,协议语句$\tau(i\to j:m)\tau'$可形式化为 $S(i,\tau,m)$及 $R(j,\tau',m)$.注意,形式化后的逻辑语句仅说明 i 在τ时发送了消息 m,j 在τ'时收到 m,但并没有对 j 所收到的 m 是否是 i 发送的作任何假设.

定义 29. 协议的初始化假设是指在分析协议之前所假设成立的前提条件,常用 S 表示协议初始假设公式集.

基于以上定义,可给出协议分析的一般过程.给定协议 $\hat{P}$,在 *TCPL* 中分析并验证其安全性的过程如下:

(1) 对 $\hat{P}$ 进行时间关联得到 P_t.

(2) 对 P_t进行形式化,得到 P.

(3) 给出初始假设公式集 S.

(4) 列出协议验证目标公式集 G.

(5) 根据 TCPL 中的公理、定理及推理规则证明协议验证目标 G 是否满足,即证明 $P\cup A\vdash_{TCPL}G$.

为了方便协议分析,以下定理可直接在分析过程中引用.在相关证明中,当用到谓词逻辑中的公理时,以“+”表示引入,“−”表示消除.如∧+表示合取引入公理,∧−表示合取消除公理.“⊥”表示矛盾,LEM(law of the excluded middle)表示排中律,PBC(proof by contradiction)表示反证法.直观起见,采用了文献[27]中在引入假设时的方框表示形式,进入方框时引入假设,出方框时消除假设.

定理 1.

(a) $B_{i,\tau}C(m,m)$.

(b) $B_{i,\tau}C([m,m'],m)\wedge B_{i,\tau}C([m,m'],m')$.

(c) $H(i,\tau,\tilde{k})\rightarrow B_{i,\tau}C([m]_k,m)$.

证明:定理 1(a):

(1) $G(i,\tau,m,m)$ A6(a)

(2) $B_{i,\tau}G(i,\tau,m,m)$ (1), IR(b)

(3) $B_{i,\tau}(\exists_a i\exists_\tau \tau G(i,\tau,m,m')\rightarrow C(m,m'))$ A7(a), IR(b)

(4) $B_{i,\tau}C(m,m)$ (2),A1, (3), A11(a)

同理可证定理 1(b).

定理 1(c):

(1)	$H(i,\tau,\tilde{k})$	假设
(2)	$B_{i,\tau}H(i,\tau,\tilde{k})$	(1), A11(d)
(3)	$B_{i,\tau}(H(i,\tau,\tilde{k})\rightarrow G(i,\tau,[m]_k,m))$	A6(b), IR(b)
(4)	$B_{i,\tau}G(i,\tau,[m]_k,m)$	(2), (3), A11(a)
(5)	$B_{i,\tau}\exists_a j\exists_\tau tG(j,t,[m]_k,m)$	∃+, IR(b), (2), A11(a)
(6)	$B_{i,\tau}(\exists_a j\exists_\tau tG(j,t,[m]_k,m)\rightarrow C([m]_k,m))$	A7(a), IR(b)
(7)	$B_{i,\tau}C([m]_k,m)$	(5), (6), A11(a)

(8) $H(i,\tau,\tilde{k})\rightarrow B_{i,\tau}C([m]_k,m)$ (1), (7), →+ □

除此之外,一些与模态逻辑中相类似的定理也可直接应用,如 $B_{i,\tau}(\varphi\rightarrow\psi)\rightarrow(B_{i,\tau}\varphi\rightarrow B_{i,\tau}\psi)$(可看作公理 A11(a)的变形)及 $B_{i,\tau}\varphi\wedge B_{i,\tau}\psi\leftrightarrow B_{i,\tau}(\varphi\wedge\psi)$等,其证明可将 $B_{i,\tau}$看作一般的模态算子参照通用的数理逻辑理论给出.

下面以 Timed-release 协议[11]和 Wide-mouthed-frog 协议[5]为例,利用 TCPL 对其进行分析.

3.2 Timed-Release协议分析

Timed-Release 协议假定有 3 个参与主体:*A*(alice),*B*(bob)及 *T*(trent).*A* 发送一消息给 *B*,并希望该消息在特定时间τ_s之前对 *A* 和 *T* 以外的任何主体保密.其中,*T* 为可信第三方,负责发放时间相关密钥.R_a 和 N_b 分别为由 *A* 生成的随机数和由 *B* 生成的现时(nonce).Timed-release 协议可描述如下:

(M1). $A\rightarrow T$:[“enc”,τ_s];

(M2). $T\rightarrow A$:[“enc”, $\tau_s, k_{\tau_s+}]_{k_T^-}$;

(M3). $A\rightarrow B$:A;

(M4). $B\rightarrow A$:N_b;

(M5). $A\rightarrow B$:$[[[X_a,R_a,A]_{k_{\tau_s+}},A,B,\tau_s,N_b,k_{\tau_s+}]_{k_A^-}$, [“enc”, $\tau_s, k_{\tau_s+}]_{k_T^-}$;

(M6). $B\rightarrow A$:$[[[X_a,R_a,A]_{k_{\tau_s+}},A,B,\tau_s,N_b,k_{\tau_s+}]_{k_A^-}]_{k_B^-}$;

(M7). $B\rightarrow T$:[“dec”,τ_s];

If *current time*$\geqslant\tau_s$,

(M8). $T\rightarrow B$:[“dec”, $\tau_s, k_{\tau_s+}]_{k_T^-}$.

以上 M*i* 表示第 *i* 个协议语句,用 m_i 表示 M*i* 中的消息.如,M1 中的消息为[“enc”,τ_s],因此可用 m_1 表示

["enc",τ_s].

在分析协议的保密性与认证性时,通常假设协议主体之间是合作关系,主体会按序执行协议,直至完成协议.因此,可根据定义 27 为协议进行时间关联,并按照协议语句的先后顺序给出时间顺序的假设.另外,如果两相邻协议语句之间的消息处理时间可忽略,可以将前者的接收时间与后者的发送时间并合为同一时间.

传统的保密性大多是指在协议结束时的保密性,而 Timed-release 协议所希望达到的实际上是一种时限保密性,即要求 X_a 在 τ_s 之前保密.以下按照 TCPL 分析协议的一般过程给出 Timed-release 协议保密性与认证性的详细分析过程:

(1) 时间关联:

忽略消息处理时间,对以上所述协议可进行如下时间关联:

T1: $\tau_0(\mathrm{M1})\tau_1$.

T2: $\tau_1(\mathrm{M2})\tau_2$.

T3: $\tau_2(\mathrm{M3})\tau_3$.

T4: $\tau_3(\mathrm{M4})\tau_4$.

T5: $\tau_4(\mathrm{M5})\tau_5$.

T6: $\tau_5(\mathrm{M6})\tau_6$.

T7: $\tau_6(\mathrm{M7})\tau_7$.

T8: $\tau_8(\mathrm{M8})\tau_9$.

由于在 τ_7 和 τ_8 之间可信第三方 T 必须检查当前时间是否大于等于 τ_s,这一时间段不能被忽略,因此用 τ_8 和 τ_9 对 M8 进行标注,而不是用 τ_7 和 τ_8.

(2) 形式化协议

P1: $S(A,\tau_0,m_1)$.

P2: $R(T,\tau_1,m_1)$.

P3: $S(T,\tau_1,m_2)$.

P4: $R(A,\tau_2,m_2)$.

P5: $S(A,\tau_2,m_3)$.

P6: $R(B,\tau_3,m_3)$.

P7: $S(B,\tau_3,m_4)$.

P8: $R(A,\tau_4,m_4)$.

P9: $S(A,\tau_4,m_5)$.

P10: $R(B,\tau_5,m_5)$.

P11: $S(B,\tau_5,m_6)$.

P12: $R(A,\tau_6,m_6)$.

P13: $S(B,\tau_6,m_7)$.

P14: $R(T,\tau_7,m_7)$.

P15: $S(T,\tau_8,m_8)$.

P16: $R(B,\tau_9,m_8)$.

(3) 初始假设

S1. 关于主体行为的假设: $(\tau<\tau_s)\wedge R(j,\tau,m)\wedge C(m,X_a)\rightarrow(\neg H(j,\tau,k_{\tau_s-})\rightarrow\neg G(j,\tau,m,X_a))$.

S1 表明,任何主体在 τ_s 之前收到了包含 X_a 的消息,如果不拥有 k_{τ_s-},则一定无法从所收到的消息中获取 X_a.换言之,在 τ_s 之前如果有主体发送消息 X_a,则一定会用 k_{τ_s+} 进行加密.

S2. 关于时间的假设:$\varphi_\tau\wedge\forall_a i\forall_\tau\tau B_{i,\tau}\varphi_\tau$.其中,$\varphi_\tau$=$((\tau_0<\tau_1<\tau_2<\tau_3<\tau_4<\tau_5<\tau_6<\tau_7<\tau_8<\tau_9)\wedge(\tau_s\leqslant\tau_8))$.

该假设表明,Timed-release 协议是按序执行的,可信第三方发布时间相关私钥的时间在 τ_s 之后,且协议的参

与者均相信这一点.

S3. 关于密钥的假设:

(a) $\forall_a i\forall_a j\forall_\tau\tau(H(i,\tau,k_j^+)\wedge\forall_a i'\forall_\tau\tau' B_{i',\tau'}\forall_a i\forall_a j\forall_\tau\tau(H(i,\tau,k_j^+)$.

(b) $H!(T,\tau_1,k_{\tau_s-})$.

其中,假设(a)表明公钥是公开的;假设(b)表明在τ_1时,只有可信第三方 T 拥有 k_{τ_s-}.

S4. 关于消息的假设:

(a) $O(X_a)\wedge H!(A,\tau_0,X_a)$.

(b) $B_{A,\tau_0}(O(X_a)\wedge H!(A,\tau_0,X_a))$.

(c) $\forall_\tau\tau((\tau_0\leqslant\tau\leqslant\tau_9)\rightarrow B_{B,\tau}\#(N_b)\wedge B_{A,\tau}\#(R_a))$.

其中:假设(a)表明,X_a是原子的,且在协议开始时只有 A 拥有 X_a;假设(b)表明,A 在协议执行之初相信假设(a);假设(c)表明,在本轮协议中,B 相信 N_b 是新鲜的,A 相信 R_a 是新鲜的.

(4) 协议目标.

G1. $\forall_\tau\tau\forall_a i((\tau<\tau_s)\wedge(i\neq_a A)\wedge(i\neq_a T)\rightarrow\neg H(i,\tau,X_a))$.

G2. $\exists_\tau\tau((\tau\geqslant\tau_s)\wedge H(B,\tau,X_a))$.

G3. $\exists_\tau\tau((\tau_0<\tau<\tau_s)\wedge B_{A,\tau}H(B,\tau,[X_a,R_a,A]_{k_{\tau_s+}}))$.

G4. $B_{B,\tau_9}\exists_\tau\tau\exists_m m((\tau_0\leqslant\tau<\tau_9)\wedge C(m,X_a)\wedge S(A,\tau,m))$.

其中,G1 和 G2 关注保密性,G3 和 G4 关注认证性.G1 表明,在τ_s之前,除了 A 和 T,没有人拥有消息 X_a.G2 表明,B 可在τ_s之后拥有消息 X_a.G3 表明,A 相信在当前协议的τ_s之前,T 拥有时间相关私钥,B 拥有以时间相关公钥加密的 X_a 的密文.G4 表明,B 相信在当前协议中的τ_s之前,A 发送过以时间相关公钥加密的 X_a 的密文.

(5) 目标证明

G1. $\forall_\tau\tau\forall_a i((\tau<\tau_s)\wedge(i\neq_a A)\wedge(i\neq_a T)\rightarrow\neg H(i,\tau,X_a))$

证明:(G1)

(1)	$t\ i'\ \ ((\tau<\tau_s)\wedge(i\neq_a A)\wedge(i\neq_a T))\ \ (t/\tau)(i'/i)$	假设
(2)	$(t<\tau_s)\wedge(i'\neq_a A)\wedge(i'\neq_a T)$	(1)
(3)	$\neg H(i',t,k_{\tau_s-})$	(2), S3(b), A5(c)
(4)	$H(i',t,X_a)$	假设
(5)	$\exists_\tau\tau\exists_a m(\tau_0<\tau'\leqslant t\wedge R(i',\tau',m)\wedge G(i',\tau',m,X_a))$	(1), (4), S4(a), A8(d)
(6)	$t_0\ m_0\quad(\tau_0<t_0<t)\wedge R(i',t_0,m_0)\wedge G(i',t_0,m_0,X_a)$	假设
(7)	$G(i',t_0,m_0,X_a)$	(6), $\wedge-$
(8)	$C(m_0,X_a)$	(7), A7(a)
(9)	$(t_0<\tau_s)\wedge R(i',t_0,m_0)\wedge C(m_0,X_a)$	(2), (6), $\wedge-$, (8), $\wedge+$
(10)	$\neg G(i',t_0,m_0,X_a)$	(9), (3), S1
(11)	$\perp$	(7), (10), $\neg-$
(12)	$\perp$	(5), (6), (11), $\exists-$
(13)	$\neg H(i',t,X_a)$	(4), (12), PBC
(14)	$(t<\tau_s)\wedge(i'\neq_a A)\wedge(i'\neq_a T)\rightarrow\neg H(i',t,X_a)$	(2), (14), $\rightarrow+$
(15)	$\forall_\tau\tau\forall_a i((\tau<\tau_s)\wedge(i\neq_a A)\wedge(i\neq_a T)\rightarrow\neg H(i,\tau,X_a))$	(1), (14), $\forall+$

□

G2. $\exists_\tau\tau((\tau\geqslant\tau_s)\wedge H(B,\tau,X_a))$

证明:

(1) $H(B,\tau_5,m_5)$	P10, A9(a)
(2) $H(B,\tau_5,k_A^+)$	S3(a), $\forall-$

(3) $G(B,\tau_5,m_5,[X_a,R_a,A]_{k_{\tau_{s^+}}})$ (2),A6(d),A6(b)

(4) $H(B,\tau_5,[X_a,R_a,A]_{k_{\tau_{s^+}}})$ (1),(3),A9(c)

(5) $H(B,\tau_9,m_8)$ P14,A9(a)

(6) $G(B,\tau_9,m_8,k_{\tau_{s^-}})$ S3(a),A6(d),A6(b)

(7) $H(B,\tau_9,k_{\tau_{s^-}})$ (5),(6),A9(c)

(8) $H(B,\tau_9,[X_a,R_a,A]_{k_{\tau_{s^+}}})$ (4),S2(a),A3(a)

(9) $H(B,\tau_9,X_a)$ (7),(8),A6,A9(c)

(10) $\tau_9 \geqslant \tau_s$ S2(a),A4(2)

(11) $\exists_\tau \tau((\tau \geqslant \tau_s) \wedge H(B,\tau,X_a))$ (9),(10),∧+,∃+ □

G3. $\exists_\tau \tau((\tau_0 < \tau < \tau_s) \wedge B_{A,\tau} H(B,\tau,[X_a,R_a,A]_{k_{\tau_{s^+}}}))$

证明:

(1) $R(A,\tau_6,[m']_{k_B^-})$,其中,$m' =_m [[X_a,R_a,A]_{k_{\tau_{s^+}}},A,B,\tau_s,N_b,k_{\tau_{s^+}}]_{k_A^-}$ P12

(2) $B_{A,\tau_6} R(A,\tau_6,[m']_{k_B^-})$ A11(c)

(3) $B_{A,\tau_6} C([m']_{k_B^-},[m']_{k_B^-})$ 定理 1(a)

(4) $H(A,\tau_6,k_B^+)$ S3(a),∀−

(5) $H(A,\tau_6,\widetilde{k_B^-})$ (4),A5(d)

(6) $B_{A,\tau_6} C([m']_{k_B^-},m')$ (5),定理 1(c)

(7) $B_{A,\tau_6}(R(A,\tau_6,[m']_{k_B^-}) \wedge C([m']_{k_B^-},[m']_{k_B^-}) \wedge C([m']_{k_B^-},m'))$ (2),(3),(5),定理 1(c),∧+,A11(a)

(8) $B_{A,\tau_6} \exists_\tau \tau\ \exists_m m((\tau < \tau_6) \wedge H(B,\tau,m'))$ (7),A8(b),IR(b),A11(a)

(9) $B_{A,\tau_6} H(B,\tau_6,m'))$ A3(a),IR(b),(8),A11(a)

(10) $B_{A,\tau_6} H(B,\tau_6,k_A^+)$ S3(a),∀−

(11) $B_{A,\tau_6} G(B,\tau_6,m',[X_a,R_a,A]_{k_{\tau_{s^+}}})$ (9),A6,IR(b),A11(a)

(12) $B_{A,\tau_6} H(B,\tau_6,[X_a,R_a,A]_{k_{\tau_{s^+}}})$ (9),(11),A9(c),IR(b)

(13) $\tau_0 < \tau_6 < \tau_s$ S2(a),A4(2)

(14) $\exists_\tau \tau((\tau_0 < \tau < \tau_s) \wedge B_{A,\tau} H(B,\tau,[X_a,R_a,A]_{k_{\tau_{s^+}}}))$ (12),(13),∧+,∃+ □

G4. $B_{B,\tau_9} \exists_\tau \tau\ \exists_m m((\tau_0 \leqslant \tau < \tau_9) \wedge C(m,X_a) \wedge S(A,\tau,m))$

证明:

(1) $B_{B,\tau_5} R(B,\tau_5,m_5)$ P10,A11(c)

(2) $B_{B,\tau_9} R(B,\tau_5,m_5)$ (1),A3(b)

(3) $B_{B,\tau_9} C(m_5,[m']_{k_A^-})$,其中,$m' =_m [[X_a,R_a,A]_{k_{\tau_{s^+}}},A,B,\tau_s,N_b,k_{\tau_{s^+}}]$ 定理 1(b)

(4) $H(B,\tau_9,k_A^+)$ S3(a)

(5) $B_{B,\tau_9} C([m']_{k_A^-},m')$ (4),定理 1(c)

(6) $B_{B,\tau_9} \exists_\tau \tau\ \exists_m m((\tau < \tau_5) \wedge C(m,m')) \wedge S(A,\tau,m))$ (2),(3),(5),A8(b),IR(b)

(7)	$t\ m_0\ \ B_{B,\tau_9}((t<\tau_5)\wedge C(m_0,m')\wedge S(A,t,m_0))$	假设
(8)	$H(B,\tau_9,k_{\tau_s-})$	G2证明步骤(7)
(9)	$B_{B,\tau_9}C(m',X_a)\wedge B_{B,\tau_9}C(m',N_b)$	(8), A11(a), A1
(10)	$B_{B,\tau_9}C(m_0,X_a)\wedge B_{B,\tau_9}C(m_0,N_b)$	(7), (9), A7(b), IR(b), A11(a)
(11)	$B_{B,\tau_9}\#(m_0)$	S4(c), (10), A10(b)
(12)	$B_{B,\tau_9}(\tau_0\leqslant t)$	(7), (11), A10(a)
(13)	$B_{B,\tau_9}((\tau_0\leqslant t<\tau_9)\wedge C(m_0,X_a)\wedge S(A,t,m_0))$	(7), (10), (12), A11(a)
(14)	$\exists_\tau\tau\ \exists_m m B_{B,\tau_9}((\tau_0\leqslant\tau<\tau_9)\wedge C(m,X_a)\wedge S(A,\tau,m))$	(13), ∃+

(15) $\forall_\tau\tau\forall_a i((\tau\prec\tau_s)\wedge(i\neq_a A)\wedge(i\neq_a T)\rightarrow\neg H(i,\tau,X_a))$ (6),(7),(14),∃−

(16) $B_{B,\tau_9}\exists_\tau\tau\exists_m m((\tau_0\leqslant\tau<\tau_9)\wedge C(m,X_a)\wedge S(A,\tau,m))$ (15),A2(b) □

从以上分析可见,Timed-release 协议满足其目标.

3.3 Wide-mouthed-frog协议分析

Wide-mouthed-frog 协议(以下简称 WMF 协议)[5]是一种使用共享密钥的密码协议,其参与者为 A,B,T,主要过程是由 A 通过 T 向 B 传递会话密钥.

WMF 协议只有两步,可在 TCPL 中表示如下:

(M1). $A\rightarrow T: A,[t_a,B,k]_{k_{AT}}$.

(M2). $T\rightarrow B:[t_t,A,k]_{k_{BT}}$.

其中,t_a 为由 A 产生的时戳,t_t 为由 T 产生的时戳,k 为会话密钥.协议规定,T 在第 1 步收到来自 A 的消息时,检验其收到消息的时间在 t_a 后的预定时间跨度(假设该时间跨度为Δ)内,然后执行协议第 2 步.B 在收到 T 发来的消息后也要检查 t_a 是否在他收到来自 T 的其他消息的接收时间之后.以下仅利用 TCPL 对 WMF 协议的认证性进行分析.

(1) 时间关联

T1: τ_0(M1)τ_1.

T2: τ_2(M2)τ_3.

(2) 形式化协议

P1: $S(A,\tau_0,m_1)$.

P2: $R(T,\tau_1,m_1)$.

P3: $S(T,\tau_2,m_2)$.

P4: $R(B,\tau_3,m_2)$.

(3) 初始假设

S1: $B_{B,\tau_3}(C(m,[t_t,A,k]_{k_{BT}})\wedge S(T,\tau,m)\rightarrow\exists_\tau\tau\exists_\tau t\exists_m m((\tau'\leqslant\tau)\wedge(t\leqslant\tau'\leqslant t+\Delta)\wedge C(m,[t,B,k]_{k_{AT}})\wedge R(T,\tau,m))$;

S2: $B_{B,\tau_3}\forall_\tau\tau\forall_\tau t\forall_m m((\tau<\tau_3)\wedge C(m,[t,A,k]_{k_{AT}})\wedge H(B,\tau,m)\wedge H(B,\tau_3,[t_t,A,k]_{k_{AT}})\rightarrow t<t_t)$.

S1,S2 是对协议两个隐式条件的形式化.

(4) 协议目标

$$B_{B,\tau_2}\exists_\tau\tau\exists_m m((\tau_0\leqslant\tau<\tau_3)\wedge C(m,[\tau,B,k]_{k_{AT}})\wedge S(A,\tau,m)).$$

(5) 目标证明

在证明前,先给出子目标: $B_{B,\tau_3}\forall_\tau\tau\forall_m m((\tau<\tau_3)\wedge C(m,[t_t,A,k]_{k_{BT}})\wedge C([t_t,A,k]_{k_{BT}},[t_t,A,k])\rightarrow\neg S(B,\tau,m))$.该子目标是说,$B$ 相信自己在τ_3之前未发送过包含 $[t_t,A,k]_{k_{BT}}$ 的消息.该子目标可由 S2 得到,因为假如 B 相信自己在τ_3之前发送过包含 $[t_t,A,k]_{k_{BT}}$ 的消息,那么由 A9(b)可知,B 相信自己在τ_3之前拥有包含 $[t_t,A,k]_{k_{BT}}$ 的消息,根据 P4 和 S2,则有 $B_{B,\tau_3}(t_t<t_t)$.而由 A4(a)和 IR(b)可证得 $B_{B,\tau_3}(t_t=_\tau t_t)$,从而得出不一致的结果.可见,该子目标成立.

以下证明协议目标.

证明:

(1) $B_{B,\tau_3}(R(B,\tau_3,m_2)\wedge C(m_2,[t_t,A,k]_{k_{BT}})\wedge C([t_t,A,k]_{k_{BT}},[t_t,A,k]))$ P4, 定理1(b), 定理1(c), A11(a)

(2) $B_{B,\tau_3}\exists_\tau\overline{\exists}_m m((\tau<\tau_3)\wedge C(m,[t_t,A,k]_{k_{BT}})\wedge(S(T,\tau,m)\vee S(B,\tau,m))$ (1), A8(c), A11(a)

(3) $\tau'\ m'$ $B_{B,\tau_3}((\tau'<\tau_3)\wedge C(m',[t_t,A,k]_{k_{BT}})\wedge(S(T,\tau',m')\vee S(B,\tau',m'))$ (2), 假设

(4) $B_{B,\tau_3}((\tau'<\tau_3)\wedge C(m',[t_t,A,k]_{k_{BT}})\wedge S(T,\tau',m'))$ (3), 子目标, $\vee-$

(5) $B_{B,\tau_3}\exists_\tau\overline{\exists}_\tau t\exists_m m((\tau\leqslant\tau')\wedge(t\leqslant\tau\leqslant t+\Delta)\wedge C(m,[t,A,k]_{k_{BT}})\wedge R(T,\tau,m))$ (4), S1, A11(a)

(6) $B_{B,\tau_3}\exists_\tau\overline{\exists}_\tau t\exists_m m((\tau_0\leqslant\tau\leqslant\tau_3)\wedge C(m,[t,A,k]_{k_{BT}})\wedge R(T,\tau,m))$ (4), S1, A11(a)

(7) $B_{B,\tau_3}\exists_\tau\overline{\exists}_\tau t\exists_m m((\tau_0\leqslant\tau\leqslant\tau_3)\wedge C(m,[t,A,k]_{k_{BT}})\wedge R(T,\tau,m))$ (3), (6), $\exists-$

(8) $\tau'\ m'$ $B_{B,\tau_3}\exists_\tau t((\tau_0\leqslant\tau'<\tau_3)\wedge C(m',[t,B,k]_{k_{AT}})\wedge R(T,\tau',m')$ (7), 假设

(9) $B_{B,\tau_3}\exists_\tau\overline{\exists}_m m\exists_\tau t((\tau<\tau')\wedge C(m,[t,B,k]_{k_{AT}})\wedge(S(A,\tau,m)\vee S(T,\tau,m))$ (8), A8(c)

(10) $B_{B,\tau 3}\exists_\tau\overline{\exists}_m m\exists_\tau t((\tau<\tau_3)\wedge C(m,[t,B,k]_{k_{AT}})\wedge(S(A,\tau,m)\vee S(T,\tau,m))$ (8), (9), A4(b)

(11) $B_{B,\tau_3}\exists_\tau\overline{\exists}_m m\exists_\tau t((\tau<\tau_3)\wedge C(m,[t,B,k]_{k_{AT}})\wedge(S(A,\tau,m)\vee S(T,\tau,m))$ (7), (8), (10),$\exists-$

以上第(11)步说明,B 相信 A 或 T 发送了包含 $[t_a,B,k]_{k_{AT}}$ 的消息,但由于无法排除 $S(T,\tau,m)$,因而也不能进一步确定 $[t,B,k]_{k_{AT}}$ 就一定出自 A.可见,Wide-mouthed-frog 不满足认证性.以上证明过程也清楚地揭示了不满足认证性的原因:T 所收到的消息很可能是 T 以前发送过的消息,即可能是被攻击者重放的消息.

文献[5]利用 BAN 逻辑简单证明了该协议的认证性.在其分析中假设 T 对 A 所发来的消息具有裁决权.但事实上,T 甚至不能确定它所收到的消息是否真的来源于 A.文献[28]给出了对 WMF 协议进行攻击的一种实例,与以上形式化分析所得出的认证性不满足原因相吻合.

4 进一步讨论

以下对 TCPL 作进一步讨论:

(1) 关于巴肯公式.由于 TCPL 采用了谓词模态逻辑,因此必须考虑量词与模态词的位置关系.从哲学的角度,它涉及到个体的跨世界识别问题[29].由于我们采用固定论域,即不同可能世界的论域相同,加上 TCPL 中所涉及的主体主要是指计算机进程,它在这一问题中有优于现实意义上的人的地方[27].因此,引入巴肯公式体现了这一思想.

(2) 关于多型变元.TCPL 采用多型变元,主要为了方便并规范逻辑语法描述.当然,也可以将其转换为单型变元,但在描述上较为累赘.

(3) 关于拥有与相信.通常的作法是采用知道与信任,前者可描述协议的保密性,后者可描述协议的认证性.然而在 TCPL 中,我们放弃使用知道模态词,代之以表达拥有的谓词 H.因为知道通常有多种意义,如知道是什么、知道是否什么、知道谁做了什么等[30],而在表达保密性时我们只关心知道是什么的问题,因此采用了拥有的概念.对于信任这一模态词时,由其语义可见,它是建立在 S5 基础上的,而在传统关于人的思维研究方面,人们乐于使用 KD45 来表达信任[31].这里,我们采纳了文献[32]中关于信任的论述,将其建立在 S5 的基础上.所不同的是,我们同时考虑了时间的因素.

(4) 关于可达关系.TCPL 中的可达关系除体现时间因素这一特点外,它与文献[9]所定义的可达关系还有一点不同的是,文献[9]在可达关系的定义中排除了不可理解的消息,在本文的定义中并未排除这类消息.原因在于,如果将消息看成比特序列,即使这一比特序列是不可理解的(如加密消息),但仍然可以通过比特序列的比较来判断任意两个此类消息之间是否有相等关系,简单地排除将无法反映这一特点.

(5) 关于发送与接收.从直观意义上来说,严格定义发送与接收可有几种方式.一是定义主体发送(或接收)了一个消息,则它发送(或接收)了所有该消息包含的消息.然而在该定义下,如果一个主体收到了以另一主体的

公钥加密的消息,则它收到了加密前的消息,从而也拥有了加密前的消息,显然这是不合理的.考虑另一种方式,定义主体发送(或接收)了一个消息,则它发送(或接收)了它可从该消息中获取的消息.这似乎可以解决前一种情况所遇到的问题,但又有新的问题出现.如,一个主体发送了以另一主体的公钥加密的消息,那么它是不能从加密的消息中获取加密前的消息的.在该定义下,只能说它发送了加密后消息,而不能说它发送了加密前的消息.但对于接收者来说,由于拥有相应的私钥,那么,它收到了以其公钥加密消息也就意味着它收到了加密前的消息,这与收到消息则必定有人发送了该消息的原则相悖.在 TCPL 中,对该问题的解决是通过引入原始消息的概念来完成的.即发送与接收仅针对原始消息,而将从原始消息中析出或重构的消息在主体所拥有的消息中体现.当然,也可以使用前两种方式来定义,但必须对由此所引起的不一致进行修改,保持逻辑的整体一致性.

(6) 关于 TCPL 的可判定性与完备性.由于谓词逻辑是半可判定的[25],因此存在 TCPL 不可判定的命题.如通常我们易于证明一个主体拥有什么,但很难证明它不拥有什么.这种情况在现有的协议逻辑中是普遍存在的.我们在 TCPL 中给出了证明“不拥有”的相关公理,表明在 TCPL 中可以证明主体不拥有什么.但这一点是有条件的,即它是以一定的初始假设为前提的.否则,这种证明将不可行.另外,对于一个逻辑系统,人们主要关心其可靠性,而并不苛求其完备性[33].我们可证明 TCPL 的可靠性,但 TCPL 并不具备完备性.如,在语义中给出了消息生成等概念,但这些在逻辑的语法中没有相对应的表述.这主要是为了保持 TCPL 的简洁性,只引入了协议验证中所必需的公理.当然,必要时也以对 TCPL 进行扩展,引入一些与现有公理相一致的公理.

(7) 关于协议验证.TCPL 可用于分析保密性、认证性以及不可否认性等属性,并且支持使用对称和非对称密码体系的密码协议,特别是对时间相关的密码协议有充分的支持.在 CS 逻辑中虽然引入了时间因素,但由于缺乏形式化语义,因此部分概念存在歧义,且无法保证所进行的分析是否可靠.另外,假设 CS 逻辑是可靠的,一些协议也无法用 CS 逻辑进行分析,如本文所给出的两个实例.

5 结束语

TCPL 基于谓词模态逻辑,形式化地定义了逻辑语言,并显式引入时间因素,充分体现了时间在密码协议中的作用;支持对密码协议保密性、认证性和不可否认性等属性的分析与验证;可分析时间相关密码协议或一般密码协议,包括对称密码及非对称密码协议;TCPL 的形式化语义基于 Kripke 结构,将可能世界建立在主体局部世界与时间局部世界的基础上,使得任一可能世界可反映协议的一个可能的全过程;该语义模型的提出在避免逻辑语言二义性的同时保证了逻辑的可靠性.下一步的工作将针对更多的密码协议,利用 TCPL 分析更多协议安全属性,如电子商务协议的公平性等.

致谢 在此,向对本文给予指导并提出宝贵意见的信息安全国家重点实验室薛锐研究员表示感谢,向在数理逻辑方面给作者以指导的解放军理工大学指挥自动化学院王元元教授和张兴元教授表示感谢.

References:

[1] Rivest RL, Shamir A, Wagner DA. Time-Lock puzzles and timed-release cryptographic protocol. Technical Report, MIT/LCS/TR-684, Cambridge: MIT Laboratory for Computer Science, 1996. 1–9.

[2] Péter T. The additional examination of the kudo-mathuria time-release protocol. Journal of Universal Computer Science, 2006, 12(9):1373−1384. [doi: 10.3217/jucs-012-09-1373]

[3] Zhang Y, Varadharajan V. A logic for modeling the dynamics of beliefs in cryptographic protocols. In: Michael O, ed. Proc. of the 24th Australasian Computer Science Conf. Washington: IEEE Computer Society, 2001. 215−222.

[4] Kim K, Park S, Back J. Improving fairness and privacy of Zhou-Gollmann’s fair non-repudiation protocol. In: Gong K, Niu Z, eds. Proc. of the 2000 IEEE Int’l Conf. on Communication. Beijing: IEEE Computer Society Press, 2000. 1743−1747.

[5] Burrows M, Abadi M, Needham R. A logic of authentication. In: Enderby JE, ed. Proc. of the Royal Society of London A, Vol.426. London: The Royal Society, 1989. 233−271. [doi: 10.1098/rspa.1989.0125]

[6] Qing SH. Twenty years development of security protocols research. Journal of Software, 2003,14(10):1740−1752 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/14/1740.htm

[7] Gong L, Needham R, Yahalom R. Reasoning about belief in cryptographic protocols. In: Cooper D, Lunt T, eds. Proc. of the '90 IEEE Computer Society Symp. on Research in Security and Privacy. Los Alamitos: IEEE Computer Society Press, 1990. 234−248. [doi: 10.1109/RISP.1990.63854]

[8] Abadi M, Tuttle MR. A semantics for a logic of authentication. In: Logrippo L, ed. Proc. of the 10th Annual ACM Symp. on Principles of Distributed Computing. New York: ACM Press, 1991. 201−216. [doi: 10.1145/112600.112618]

[9] Syverson PF, van Oorschot PC. On unifying some cryptographic protocol logics. In: Rushby J, Meadows C, eds. Proc. of the '94 IEEE Computer Society Symp. on Research in Security and Privacy. Oakland: IEEE Computer Society Press, 1994. 14−28. [doi: 10.1145/112600.112618]

[10] Coffey T, Saidha P. Logic for verifying public-key cryptographic protocols. IEEE Proc. of Computers and Digital Techniques, 1997, 144(1):28−32. [doi: 10.1049/ip-cdt:19970838]

[11] Michiharu K, Anish M. An extended logic for analyzing timed-release public-key protocols. In: Vijay V, Yi M, eds. Proc. of the 2nd Int'l Conf. on Information and Communication Security. LNCS 1726, New York: Springer-Verlag, 1999. 183−198. [doi: 10.1007/978-3-540-47942-0_16]

[12] Lei XF, Xiao JM, Liu J, Wang YB. A logic for analyzing time-dependent cryptographic protocol. In: Li MQ, ed. Proc. of the 2nd Int'l Conf. on Computer Science and Education. Xiamen: Xiamen University Press, 2007. 853−858.

[13] Syverson PF. Adding time to logic of authentication. In: Denning D, Pyle R, Ganesan R, Sandhu R, Ashby V, eds. Proc. of the 1st ACM Conf. on Computer and Communications Security. New York: ACM Press, 1993. 97−101. [doi: 10.1145/168588.168600]

[14] Clare D, Mari-Carmen FG, Michael F, Wiebe H. Temporal logics of knowledge and their applications in security. Electronic Notes in Theoretical Computer Science, 2007,186:27−42. [doi: 10.1016/j.entcs.2006.11.043]

[15] Christian H, Alan J. Timed Spi-calculus with types for secrecy and authenticity. In: Abadi M, Alfaro L, eds. Proc. of the CONCUR 2005—Concurrency Theory. LNCS 3653, Berlin: Springer-Verlag, 2005. 202−216. [doi: 10.1007/11539452_18]

[16] Julien C, Benoit L, Jean-Jacques Q. Efficient and non-interactive timed-release encryption. In: Qing SH, Mao WB, Lopez J, Wang GL, eds. Proc. of the 7th Int'l Conf. on Information and Communications Security. LNCS 3783, Berlin: Springer-Verlag, 2005. 291−303. [doi: 10.1007/11602897_25]

[17] Jakubowska G, Penczek W. Modeling and checking timed authentication of security protocols. Fundamenta Informaticae, 2007, 79(3-4):363−378.

[18] Corin R, Etalle S, Hartel PH, Mader A. Timed analysis of security protocols. Journal of Computer Security, 2007,15(6):619−645.

[19] Liang J, Ao QY, You JY. Analyzing the temporal accountability of secure protocols. Acta Electronica Sinica, 2002,30(10):1−5 (in Chinese with English abstract).

[20] Fan H, Feng DG. An extension logic of timed-release public key protocols analysis. Chinese Journal of Computers, 2003,26(7): 831−836 (in Chinese with English abstract).

[21] Zhao HW, Li DX, Qin J. Time-Dependent extension logic of secure protocols. Computer Applications, 2005,25(10):2272−2275 (in Chinese with English abstract).

[22] Zhou J, Gollmann D. A fair non-repudiation protocol. In: Rosch-Eisen M, Senban C, eds. Proc. of the 1996 IEEE Symp. on Security and Privacy. Oakland: IEEE Computer Press, 1996. 55−61. [doi: 10.1109/SECPRI.1996.502669]

[23] Li BT, Luo JZ. Formal analysis of timelyness in non-repudiation protocols. Journal of Software, 2006,17(7):1510−1516 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/17/1510.htm [doi: 10.1360/jos171510]

[24] Feng DG, Fan H. Survey on theories and methods of formal analyses for security protocols. Journal of the Graduate School of the Chinese Academy of Sciences, 2003,20(4):389−406 (in Chinese with English abstract).

[25] Wang YY. Modern Logic in Computer Science. Beijing: Science Press, 2001. 28−47 (in Chinese).

[26] Boolos GS, Burgess JP, Jeffrey RC. Computability and Logic. 4th ed., Cambridge: Cambridge University Press, 2002. 114−119.

[27] Michael H, Mark R. Logic in Computer Science—Modelling and Reasoning about Systems. 2nd ed., Cambridge: Cambridge University Press, 2004. 331−350.

[28] John C, Jeremy J. A survey of authentication protocol literature. Version 1.0. 1997. http://www.cs.york.ac.uk/~jac/papers/drareviewps.ps.

[29] Zhu SL. Research on Logic Semantics. Shanghai: Shanghai Educational Publishing House, 1992. 144−190 (in Chinese).

[30] Benthem J. Open problem in logical dynamics. In: Dov MG, Sergei SG, Michael Z, eds. Proc. of the Mathematical Problems from Applied Logic I. New York: Springer-Verlog, 2006. 137−192.

[31] Wiebe VD. Systems for knowledge and belief. Logic Computer, 1993,3(2):173−195. [doi: 10.1093/logcom/3.2.173]

[32] Syverson PF. The use of logic in the analysis of cryptographic protocols. In: Proc. of the 1991 IEEE Symp. on Security and Privacy. Oakland: IEEE Computer Press, 1991. 156−170. [doi: 10.1109/RISP.1991.130784]

[33] Xue R, Feng DG. The approaches and technologies for formal verification of security protocols. Chinese Journal of Computers, 2006,29(1):1−20 (in Chinese with English abstract).

附中文参考文献:

[6] 卿斯汉.安全协议 20 年研究进展.软件学报,2003,14(10):1740−1752. http://www.jos.org.cn/1000-9825/14/1740.htm

[19] 梁坚,敖青云,尤晋元.安全协议的时限责任分析.电子学报,2002,30(10):1−5.

[20] 范红,冯登国.一种分析 Timed-Release 公钥协议的扩展逻辑.计算机学报,2003,26(7):831−836.

[21] 赵华伟,李大兴,秦静.一种时间相关的分析密码协议的扩展逻辑.计算机应用,2005,25(10):2272−2275.

[23] 黎波涛,罗军舟.不可否认协议时限性的形式化分析.软件学报,2006,17(7):1510−1516. http://www.jos.org.cn/1000-9825/17/1510.htm [doi: 10.1360/jos171510]

[24] 冯登国,范红.安全协议形式化分析理论与方法研究综述.中国科学院研究生院学报,2003,20(4):389−406.

[25] 王元元.计算机科学中的现代逻辑学.北京:科学出版社,2001.28−47.

[29] 朱水林.逻辑语义学研究.上海:上海教育出版社,1992.144−190.

[33] 薛锐,冯登国.安全协议的形式化分析技术与方法.计算机学报,2006,29(1):1−20.

附录:TCPL 的可靠性

对于一个逻辑系统来说,可靠性是其最重要的属性,它保证了在逻辑语法范畴内通过推理而得到的结论在语义的范畴内也是有效的.在证明 TCPL 的可靠性之前,首先给出一些相关的定义及定理.

定义 30. 称公式φ是 TCPL 的定理,记为$\vdash_{TCPL}\varphi$(以下简记为$\vdash\varphi$),当且仅当存在一个 TCPL 中的公式序列$\varphi_1\varphi_2\ldots\varphi_i\ldots\varphi_n$使得$\varphi_n=\varphi$,且$\varphi_i(1\leqslant i\leqslant n)$或者是 TCPL 的公理,或者是由$\varphi_j,\varphi_k(j<i,k<i)$通过 TCPL 的推理规则得出,并称$\varphi_1\varphi_2\ldots\varphi_i\ldots\varphi_n$为公式$\varphi$的证明序列.

定义 31. 称公式φ在 TCPL 中由公式集Γ可推演,记为$\Gamma\vdash_{TCPL}\varphi$(简记为$\Gamma\vdash\varphi$),当且仅当存在一个 TCPL 中的公式序列$\varphi_1\varphi_2\ldots\varphi_i\ldots\varphi_n$使得$\varphi_n=\varphi$,且$\varphi_i(1\leqslant i\leqslant n)$或者是$\Gamma$中的公式,或者 TCPL 的公理,或者是由$\varphi_j,\varphi_k(j<i,k<i)$通过 TCPL 的推理规则得出.这时,也称$\varphi$为$\Gamma$的语法后承.

定义 32. 称公式φ在模型$\mathcal{M}$中是有效的,记为$\models_{\mathcal{M}}\varphi$(简记为$\models\varphi$),当且仅当对所有可能世界$\omega\in W$,有$\models^{\omega}_{\mathcal{M}}\varphi$.

定义 33. 称公式φ是公式集Γ的语义后承,记为$\Gamma\models\varphi$,当且仅当如果所有$\gamma\in\Gamma$是有效的,则φ是有效的.

在密码协议的验证中,通常Γ为协议的形式化公式集及初始假设公式集.

定理 2. 对任一可能世界$\omega\in W,\tau_1\in T,\tau_2\in T$,如果$\tau_1\leqslant\tau_2$,则,

(1) $M_i^{\tau_1}(\omega)\subseteq M_i^{\tau_2}(\omega)$.

(2) $K_i^{\tau_1}(\omega)\subseteq K_i^{\tau_2}(\omega)$.

定理 2 可由定义 13 中状态转换函数的定义立即可得.

定理 3. 对任意消息集合 M 及密钥集合 K,有 $extract_K(M)\subseteq construct_K(M)$.

定理 3 由定义 11(1)~定义 11(3)及定义 12(1)~定义 12(3)的对应性立即可得.

定理 4. 对任意消息 $m\in M$ 及密钥集合 K,如果不存在 $m',m''\in M,k\in K$ 使得 $m=_m[m',m'']$或 $m=_m[m']_k$,且$m\in construct_K(M)$,则 $m\in extract_K(M)$.

证明:由定义 12 可知,对任意 $m\in construct_{K'}(M)$,m 能够由 M 中的消息经过若干次的变形(分拆、组合、加密

或解密)而得到,设在构造 m 的过程中,第 j 次变形所构造的消息为 $m^{(j)}$.以下通过对变形的次数 n(即 $m=m^{(n)}$)进行归纳来证明 $m\in extract_K(M)$.

当 $n=0$ 时,$m\in M$.由定义 11(1)知,$m\in extract_K(M)$.

设当 $n=j$ 时有 $m^{(j)}\in extract_K(M)$,则当 $n=j+1$ 时分两种情况(根据前提可排除定义 12(4)、定义 12(5)两种情况):

(i) 存在 m''使得 $m^{(j)}=\{m^{(j+1)},m''\}$或 $m^{(j)}=[m'',m^{(j+1)}]$.由定义 11(2)有 $m^{(j+1)}\in extract_K(M)$,即 $m\in extract_K(M)$;

(ii) 存在 $k\in K$ 或 $k\in extract_K(M)$使得 $m^{(j)}=[m^{(j+1)}]_k$,由定义 11(3)知 $m^{(j+1)}\in extract_K(M)$,即 $m\in extract_K(M)$. □

定理 5. 对任意消息集合 M,M'及密钥集合 K,K',如果 $M'\subseteq M$,且 $K'\subseteq K$,则,

(1) $extract_{K'}(M')\subseteq extract_K(M)$.

(2) $construct_{K'}(M')\subseteq construct_K(M)$.

证明:

(1) 类似于定理 4 的证明方法,以下通过对变形的次数 n(即 $m=m^{(n)}$)进行归纳来证明:

$$extract_{K'}(M')\subseteq extract_K(M).$$

对任意 $m\in extract_{K'}(M')$,当 $n=0$ 时,显然有 $m\in M'$.由于 $M'\subseteq M$,因此 $m\in M$.由定义 11(1)知 $m\in extract_K(M)$,从而 $extract_{K'}(M')\subseteq extract_K(M)$;

设当 $n=j$ 时有 $extract_{K'}(M')\subseteq extract_K(M)$,则当 $n=j+1$ 时,分两种情况:

(i) 存在 m'使 $m^{(j)}=[m^{(j+1)},m']\in extract_{K'}(M')$或 $m^{(j)}=[m',m^{(j+1)}]\in extract_{K'}(M')$,则有$[m^{(j+1)},m']\in extract_K(M)$或$[m',m^{(j+1)}]\in extract_K(M)$.由定义 11(2)有 $m^{(j+1)}\in extract_K(M)$,即 $m\in extract_K(M)$,因此 $extract_{K'}(M')\subseteq extract_K(M)$.

(ii) 存在 $\tilde{k}\in K'$ 或 $\tilde{k}\in extract_{K'}(M')$,且有 $m^{(j)}=[m^{(j+1)}]_k\in extract_{K'}(M')$,则有 $\tilde{k}\in K$ 或 $\tilde{k}\in extract_K(M)$,且 $m^{(j)}=[m^{(j+1)}]_k\in extract_K(M)$.由定义 11(3)知 $m^{(j+1)}\in extract_K(M)$,即 $m\in extract_K(M)$,因此 $extract_{K'}(M')\subseteq extract_K(M)$.

(2) 类似于定理 5(1)的证明方法,通过对变形的次数 n(即 $m=m^{(n)}$)进行归纳来证明:

$$construct_{K'}(M')\subseteq construct_K(M).$$

对任意 $m\in construct_{K'}(M')$,当 $n=0$ 时显然有 $m\in M'$.由于 $M'\subseteq M$,因此 $m\in M$.由定义 12(1)知 $m\in construct_K(M)$,从而 $construct_{K'}(M')\subseteq construct_K(M)$;

设当 $n=j$ 时有 $construct_{K'}(M')\subseteq construct_K(M)$,则当 $n=j+1$ 时分 4 种情况:

情况(i)、情况(ii)与上述证明定理 5(1)中的情况(i)、情况(ii)类似,可比照定理 5(1)给出证明,此处略去.

(iii) 存在 $m'\in construct_{K'}(M')$ 使得 $m^{(j+1)}=[m^{(j)},m']$ 或 $m^{(j+1)}=[m',m^{(j)}]$, 则 $m'\in construct_K(M)$. 又由于 $m^{(j)}\in construct_{K'}(M')$,由定义 12(4)有 $m^{(j+1)}\in construct_K(M)$,即 $m\in construct_K(M)$,因此,

$$construct_{K'}(M')\subseteq construct_K(M).$$

(iv) 存在 $k\in K'$或 $k\in extract_{K'}(M')$使得 $m^{(j+1)}=[m^{(j)}]_k$,则 $k\in K$ 或 $k\in extract_K(M)$(根据定理 5(1)的结论),由定义 12(5)知 $m^{(j+1)}\in construct_K(M)$,即 $m\in construct_K(M)$,因此 $construct_{K'}(M')\in construct_K(M)$. □

推论 1. 对任一可能世界$\omega\in W,\tau_1\in T,\tau_2\in T$,如果$\tau_1\leqslant\tau_2$,则,

$$construct_{K_i^{\tau_1}(\omega)}(M_i^{\tau_1}(\omega))\subseteq construct_{K_i^{\tau_2}(\omega)}(M_i^{\tau_2}(\omega)).$$

推论 1 由定理 2 及定理 5(2)可得.

定理 6. 对任意 $m\in M$ 及密钥集合 K,有

$$extract_K(m)\subseteq contain(m).$$

定理 6 可由定义 10、定义 11 用类似于定理 4 的归纳法证明(具体证明过程略).

定理 7. 如果 $\sigma_i^{\tau}(\omega_1)=\sigma_i^{\tau}(\omega_2)$,则对任意的$\tau',\tau_0\leqslant\tau'\leqslant\tau$,有

$$\sigma_i^{\tau'}(\omega_1)=\sigma_i^{\tau'}(\omega_2).$$

证明:设 $\sigma_i^{\tau}(\omega_1)=\alpha_i^{\tau_0}(\omega_1)\alpha_i^{\tau_1}(\omega_1)...\alpha_i^{\tau}(\omega_1),\sigma_i^{\tau}(\omega_2)=\alpha_i^{\tau_0}(\omega_2)\alpha_i^{\tau_1}(\omega_2)...\alpha_i^{\tau}(\omega_2)$,根据定义 19,由于 $\sigma_i^{\tau}(\omega_1)=\sigma_i^{\tau}(\omega_2)$,$\tau_0\leqslant\tau'\leqslant\tau$,因此有 $\alpha_i^{\tau'}(\omega_1)=\alpha_i^{\tau'}(\omega_2)$,从而对任意的 $\tau'',\tau_0\leqslant\tau''\leqslant\tau'$ 有 $\alpha_i^{\tau''}(\omega_1)=\alpha_i^{\tau''}(\omega_2)$.根据定义 19,有 $\sigma_i^{\tau'}(\omega_1)=\sigma_i^{\tau'}(\omega_2)$. □

定理 8. 对任一可能世界$\omega\in W,\tau\in T,\tau'\in T$且$\tau'\geqslant\tau$,则

$$\{\omega'\mid\omega R_i^{\tau'}\omega'\}\subseteq\{\omega''\mid\omega R_i^{\tau}\omega''\}.$$

证明:假设$\omega_1\in\{\omega'\mid\omega R_i^{\tau'}\omega'\}$,则有$\omega R_i^{\tau'}\omega_1$.由定义 20 知$\omega_i^{\tau'}=(\omega_1)_i^{\tau'}$,即$(q_i^{\tau_0}(\omega),\sigma_i^{\tau'}(\omega))=(q_i^{\tau_0}(\omega_1),\sigma_i^{\tau'}(\omega_1))$,从而$\sigma_i^{\tau'}(\omega)=\sigma_i^{\tau'}(\omega_1)$.又由于$\tau'\geqslant\tau$,由定理 7 可知,$\sigma_i^{\tau}(\omega)$=$\sigma_i^{\tau}(\omega_1)$,因此$(q_i^{\tau_0}(\omega),\sigma_i^{\tau}(\omega))=(q_i^{\tau_0}(\omega_1),\sigma_i^{\tau}(\omega_1))$,即$\omega_i^{\tau}=(\omega_1)_i^{\tau}$.从而$\omega R_i^{\tau}\omega_1$,即$\omega_1\in\{\omega''\mid\omega R_i^{\tau}\omega''\}$,由此得出$\{\omega'\mid\omega R_i^{\tau'}\omega'\}\subseteq\{\omega''\mid\omega R_i^{\tau}\omega''\}$成立. □

定理 9. 对任一可能世界$\omega\in W,\tau\in T,i\in A$,如果 i 在τ时首发了消息$[m]_k$,则

$$m\in construct_{K_i^{\tau}(\omega)}M_i^{\tau}(\omega)且k\in K_i^{\tau}(\omega).$$

证明:假设$m\notin construct_{K_i^{\tau}(\omega)}M_i^{\tau}(\omega)$或$k\notin K_i^{\tau}(\omega)$,由定义 12 及定义 13(3)可知,$i$ 在τ之前收到过包含$[m]_k$的消息.这与 i 在τ时首发了消息$[m]_k$矛盾,从而定理成立. □

定理 10. 对任一可能世界$\omega\in W$,如果$[m]_{k_j^-}\in contain(m')$且$receive(m')\in\sigma_i^{\tau}(\omega)$,则存在$\tau'<\tau$,使得 j 在τ'时首发了消息$[m]_{k_j^-}$.

证明:假设$[m]_{k_j^-}$不是由 j 首发的,则一定存在非 j 的主体首发了$[m]_{k_j^-}$.不妨设 i'在τ'时首发了$[m]_{k_j^-}$,且有$\vDash_{\mathcal{M}}^{\omega} i'\neq_a j$.由定理 9 知$k_j^-\in K_{i'}^{\tau'}(\omega)$,与私钥的定义矛盾.以下证明$\tau'<\tau$.假设$\tau'\geqslant\tau$,由定义 15 知,不存在主体在$\tau$之前发送过包含$[m]_{k_j^-}$的消息,但已知 i 在τ时收到了包含$[m]_{k_j^-}$的消息,与定义 18(1)矛盾.综合以上知,存在$\tau'<\tau$,使得 j 在τ'时首发了消息$[m]_{k_j^-}$. □

定理 11. 对任一可能世界$\omega\in W$,如果$[m]_{k_{ij}}\in contain(m')$且$receive(m')\in\sigma_i^{\tau}(\omega)$且,则存在$\tau'<\tau$,使得 i 或 j 在τ'时首发了消息$[m]_{k_{ij}}$.

定理 11 的证明与定理 10 类似,此处略去.

定理 12. 对任一可能世界$\omega\in W,i\in A,\tau\in T$,关于$construct_{K_i^{\tau}(\omega)}M_i^{\tau}(\omega)$有如下结论:

(1) 当 m 为原子消息时$m\in construct_{K_i^{\tau}(\omega)}M_i^{\tau}(\omega)$,当且仅当以下条件之一成立:

(i) $generate(m)\in\sigma_i^{\tau}(\omega)$.

(ii) 存在 m',使得$receive(m')\in\sigma_i^{\tau}(\omega)$且$m\in extract_{K_i^{\tau}(\omega)}(m')$.

(2) 加密消息$[m]_k\in construct_{K_i^{\tau}(\omega)}M_i^{\tau}(\omega)$,当且仅当以下条件之一成立:

(i) 存在 m',使得$receive(m')\in\sigma_i^{\tau}(\omega)$且$[m]_k\in extract_{K_i^{\tau}(\omega)}(m')$.

(ii) $m\in construct_{K_i^{\tau}(\omega)}M_i^{\tau}(\omega)$且$k\in construct_{K_i^{\tau}(\omega)}M_i^{\tau}(\omega)$.

(3) 组合消息$[m,m']\in construct_{K_i^{\tau}(\omega)}M_i^{\tau}(\omega)$,当且仅当$m\in construct_{K_i^{\tau}(\omega)}M_i^{\tau}(\omega)$且$m'\in construct_{K_i^{\tau}(\omega)}M_i^{\tau}(\omega)$.

以上结论由定义 11、定义 12、定义 13(3)不难证明,详细证明略.

定理 13. TCPL 的所有公理是有效的.

证明:设$\omega\in W$为任一可能世界,以下对 TCPL 中的公理有效性进行逐个证明:

A1. 由谓词逻辑的可靠性以及算术公理系统的可靠性立即可得 A1 是有效的.

A2. 由于$\mathcal{M}$中的论域是固定的,即所有可能世界共享相同的论域,因此由谓词模态逻辑的理论可知,A2 在$\mathcal{M}$中有效.

A3(a). $H(i,\tau,m)\rightarrow\forall_{\tau}\tau'((\tau'\geqslant\tau)\rightarrow H(i,\tau',m))$.

假设$\vDash_{\mathcal{M}}^{\omega} H(i,\tau,m)$,由定义 25(4)可知,$\overline{s}(m)\in construct_{K_{\overline{s}(i)}^{\overline{s}(\tau)}(\omega)}(M_{\overline{s}(i)}^{\overline{s}(\tau)}(\omega))$;对任意$\iota\in T$,设$\iota\geqslant\overline{s}(\tau)$,由推论 1 可知,$\overline{s}(m)\in construct_{K_{\overline{s}(i)}^{\iota}(\omega)}(M_{\overline{s}(i)}^{\iota}(\omega))$.根据定义 25(4)、定义 25(11)有$\vDash_{\mathcal{M}}^{\omega}\forall_{\tau}\tau'((\tau'\geqslant\tau)\rightarrow H(i,\tau',m))$,该公理有效.

A3(b). $B_{i,\tau}\varphi\rightarrow\forall_{\tau}\tau'((\tau'\geqslant\tau)\rightarrow B_{i,\tau'}\varphi)$.

假设 $\vDash_{\mathcal{M}}^{\omega} B_{i,\tau}\varphi$,由定义 25(12)可知,对任一$\omega'\in W$,如果 $\omega R_{\overline{s}(i)}^{\overline{s}(\tau)}\omega'$,则有 $\vDash_{\mathcal{M}}^{\omega'}\varphi$.即对所有 $\{\omega'\mid\omega R_{\overline{s}(i)}^{\overline{s}(\tau)}\omega'\}$ 中的可能世界ω',有 $\vDash_{\mathcal{M}}^{\omega'}\varphi$.对任意$\iota\in T$,设 $\iota\geqslant\overline{s}(\tau)$,由定理 8 知 $\{\omega'\mid\omega R_{\overline{s}(i)}^{\overline{s}(\tau)}\omega'\}\supseteq\{\omega''\mid\omega R_{\overline{s}(i)}^{\iota}\omega''\}$.从而对所有 $\{\omega''\mid\omega R_{\overline{s}(i)}^{\iota}\omega''\}$ 中的可能世界ω',有 $\vDash_{\mathcal{M}}^{\omega''}\varphi$.由定义 25(11)、定义 25(12)知 $\vDash_{\mathcal{M}}^{\omega}\forall_{\tau}\tau'((\tau'\geq\tau)\rightarrow B_{i,\tau'}\varphi)$,该公理有效.

A4(a),A4(b)的有效性由定义 9(2)及定义 25(1)立即可得.

A5 中各公理的有效性由定义 9(3)立即可得.

A6(a),A6(b)的有效性由定义 11 及定义 25(3)立即可得其有效性.

A6(c). $H(i,\tau,\tilde{k})\rightarrow G(i,\tau,[m]_k,m)$.

假设 $\vDash_{\mathcal{M}}^{\omega} H(i,\tau,\tilde{k})$,由定义 25(4)知 $\overline{s}(\tilde{k})\in construct_{K_{\overline{s}(i)}^{\overline{s}(\tau)}(\omega)}(M_{\overline{s}(i)}^{\overline{s}(\tau)}(\omega))$.考虑到密钥的原子性,由定理 4 知 $\overline{s}(\tilde{k})=\widetilde{\overline{s}(k)}\in extract_{K_{\overline{s}(i)}^{\overline{s}(\tau)}(\omega)}(M_{\overline{s}(i)}^{\overline{s}(\tau)}(\omega))$,由定义 11(1)知 $\overline{s}([m]_k)\in extract_{K_{\overline{s}(i)}^{\overline{s}(\tau)}(\omega)}(\overline{s}([m]_k))$.根据定义 11(3),有

$$\overline{s}(m)\in extract_{K_{\overline{s}(i)}^{\overline{s}(\tau)}(\omega)}(\overline{s}([m]_k)).$$

从而,由定义 25(2)知 $\vDash_{\mathcal{M}}^{\omega} G(i,\tau,[m]_k,m)$.

A6(d)的有效性由定义 11 及定义 25(3)立即可得.

A7(a)的有效性由定义 25(2)、定义 25(3)及定理 6 立即可得.

A7(b)的有效性由定义 10 及定义 25(2)立即可得.

A8(a)的有效性由定义 18(1)及定义 13(2)立即可得.

A8(b). $R(i,\tau,m)\wedge C(m,[m']_{k_j^-})\wedge C([m']_{k_j^-},m')\rightarrow\exists_{\tau}\tau\exists_m m''((\tau'<\tau)\wedge C(m'',m')\wedge S(j,\tau',m'')\wedge H(j,\tau',m'))$.

假设 $\vDash_{\mathcal{M}}^{\omega} R(i,\tau,m)\wedge C(m,[m']_{k_j^-})\wedge C([m']_{k_j^-},m')$,由定理 10 知 $\overline{s}(j)$在$\overline{s}(\tau)$之前时首发了消息 $\overline{s}([m]_{k_j^-})$.由定义 15 知 $\vDash_{\mathcal{M}}^{\omega}\exists_{\tau}\tau\exists_m m''((\tau'<\tau)\wedge C(m'',[m]_{k_j^-})\wedge S(j,\tau',m''))$.由定理 9 知 $\overline{s}(m')\in construct_{K_{\overline{s}(i)}^{\overline{s}(\tau)}(\omega)}M_{\overline{s}(i)}^{\overline{s}(\tau)}(\omega)$,即 $\vDash_{\mathcal{M}}^{\omega} H(i,\tau,m')$.由 $\vDash_{\mathcal{M}}^{\omega} C(m'',[m]_{k_j^-})$及 $\vDash_{\mathcal{M}}^{\omega} C([m]_{k_j^-},m)$知 $\vDash_{\mathcal{M}}^{\omega} C(m'',m)$.从而有

$$\vDash_{\mathcal{M}}^{\omega}\exists_{\tau}\tau'\ \exists_m m''((\tau'<\tau)\wedge C(m'',m')\wedge S(j,\tau',m'')\wedge H(j,\tau',m')).$$

A8(c)的有效性可通过定理 11,并用类似于定理 10 的方法证明.

A8(d)的有效性证明可分为以下两步:

(1) $O(m)\wedge(j\neq_a i)\wedge H!(j,\tau,m)\wedge H(j,\tau',m)\rightarrow\exists_m m'\exists_{\tau}\tau''((\tau<\tau''\leqslant\tau')\wedge R(j,\tau'',m')\wedge G(j,\tau'',m',m))$.

假设 $\vDash_{\mathcal{M}}^{\omega} O(m)\wedge(j\neq_a i)\wedge H!(i,\tau,m)\wedge H(j,\tau',m)$,则$\overline{s}(m)$为原子消息,且 $\overline{s}(j)$在$\overline{s}(\tau)$时不拥有 $\overline{s}(m)$,而在 $\overline{s}(\tau')$时拥有 $\overline{s}(m)$.由 A3(a)的有效性知 $\overline{s}(\tau)<\overline{s}(\tau')$,由定义 25(3)、定义 25(4)及定理 12(1)知,$\overline{s}(j)$在$\overline{s}(\tau)$至$\overline{s}(\tau')$期间或者生成了 $\overline{s}(m)$,或者收到了它可以从中获取 $\overline{s}(m)$ 的消息.由定义 13(2)(iii)可知,消息在被生成之前不可能有主体拥有它,从而 $\overline{s}(j)$ 不可能生成 $\overline{s}(m)$,因此后者成立.另外,考虑到 $\overline{s}(j)$ 的接收行为不可能在τ时(否则$H!(i,\tau,m)$将不成立),所以步骤(1)有效.

(2) $O(m)\wedge(j\neq_a i)\wedge H!(j,\tau,m)\wedge H(j,\tau',m)\rightarrow\exists_m m'\exists_{\tau}\tau''((\tau<\tau''\leqslant\tau')\wedge S(j,\tau'',m')\wedge C(m',m))$.

假设 $\vDash_{\mathcal{M}}^{\omega} O(m)\wedge(j\neq_a i)\wedge H!(i,\tau,m)\wedge H(j,\tau',m)$,由上述步骤(1)知 $\vDash_{\mathcal{M}}^{\omega}\exists_m m'\exists_{\tau}\tau''((\tau<\tau''\leqslant\tau')\wedge R(j,\tau'',m')\wedge G(j,\tau'',m',m))$,从而 $\vDash_{\mathcal{M}}^{\omega} C(m',m)$.由 A8(a)的有效性知,存在主体在 $\overline{s}(\tau'')$ 之前发送过包含 $\overline{s}(m)$ 的消息.如果能证明 $\overline{s}(m)$ 是由 $\overline{s}(i)$ 首发的,则根据定义 15 及定义 18(2)可得步骤(2)的有效性.以下证明 $\overline{s}(m)$ 是由 $\overline{s}(i)$在$\overline{s}(\tau'')$之前首发的.假设 $\overline{s}(m)$ 不是由 $\overline{s}(i)$在$\overline{s}(\tau'')$之前首发的,则一定存在非 $\overline{s}(i)$ 的主体在 $\overline{s}(\tau'')$ 之前首发了 $\overline{s}(m)$.不妨设该主体为 $\overline{s}(i')$,且有 $\vDash_{\mathcal{M}}^{\omega} i'\neq_a i$,则由定义 18(2)有,$\overline{s}(i')$在$\overline{s}(\tau'')$之前拥有 $\overline{s}(m)$.这与 $\vDash_{\mathcal{M}}^{\omega} H!(i,\tau,m)$ 矛盾.

综合步骤(1)、步骤(2)可得 A8(d)的有效性.

A8(e). $\neg H(i,\tau,k)\wedge H(i,\tau,[m]_k)\rightarrow\exists_{\tau}\tau'\exists_m m'((\tau'<\tau)\wedge R(i,\tau',m')\wedge G(i,\tau,m',[m]_k))$.

假设 $\vDash_{\mathcal{M}}^{\omega}\neg H(i,\tau,k)\wedge H(i,\tau,[m]_k)$,则有 $\vDash_{\mathcal{M}}^{\omega} H(i,\tau,[m]_k)$.由定义 25(4)可知,$\overline{s}([m]_k)\in construct_{K_{\overline{s}(i)}^{\overline{s}(\tau)}}M_{\overline{s}(i)}^{\overline{s}(\tau)}$;由定理 12(2)知,存在以下两种可能:

(i) 存在 m',使得 $receive(m')\in\sigma_i^{\tau}(\omega)$且$[m]_k\in extract_{K_i^{\tau}(\omega)}(m')$;

(ii) $m\in construct_{K_i^{\tau}(\omega)}M_i^{\tau}(\omega)$且$k\in construct_{K_i^{\tau}(\omega)}M_i^{\tau}(\omega)$.

由$\vDash_{\mathcal{M}}^{\omega}\neg H(i,\tau,k)$知,情况(i)是不可能的,因此情况(ii)成立.根据定义 25(3)、定义 25(6)有

$$\vDash_{\mathcal{M}}^{\omega}\exists_{\tau}\tau\exists_{m}m'((\tau'<\tau)\wedge R(i,\tau',m')\wedge G(i,\tau,m',[m]_k)).$$

A9(a)的有效性由定义 12(3)、定义 11 及定义 25(4)立即可得.

A9(b)的有效性由定义 18(2)立即可得.

A9(c). $H(i,\tau,m)\wedge G(i,\tau,m,m')\rightarrow H(i,\tau,m')$.

假设$\vDash_{\mathcal{M}}^{\omega}H(i,\tau,m)\wedge G(i,\tau,m,m')$,则由定义 25(3)、定义 25(4)可知,

$$\overline{s}(m)\in construct_{K_{\overline{s}(i)}^{\overline{s}(\tau)}(\omega)}(M_{\overline{s}(i)}^{\overline{s}(\tau)}(\omega)),s(m')\in extract_{K_{\overline{s}(i)}^{\overline{s}(\tau)}(\omega)}(\overline{s}(m)).$$

由定理 3 可知,$\overline{s}(m')\in construct_{K_{\overline{s}(i)}^{\overline{s}(\tau)}(\omega)}(s(m))$,由定理 5(2)知$\overline{s}(m')\in construct_{K_{\overline{s}(i)}^{\overline{s}(\tau)}(\omega)}(M_{\overline{s}(i)}^{\overline{s}(\tau)}(\omega))$.从而根据定义 25(4),有$\vDash_{\mathcal{M}}^{\omega}H(i,\tau,m')$.

A9(d)的有效性由定义 25(4)及定义 12(4)立即可得.

A9(e)的有效性由定义 25(4)、定理 4 及定义 12(5)立即可得.

A10(a)、A10(b)新鲜性公理由定义 25(7)立即可得.

A11(a). $B_{i,\tau}\varphi\wedge B_{i,\tau}(\varphi\rightarrow\psi)\rightarrow B_{i,\tau}\psi$的有效性可由定义 25(12)及标准模态逻辑的结论立即可得.

A11(b). $S(i,\tau,m)\rightarrow B_{i,\tau}S(i,\tau,m)$.

假设$\vDash_{\mathcal{M}}^{\omega}S(i,\tau,m)$,即 $send(m)\in\alpha_{s(i)}^{s(\tau)}(\omega)$,则对任意$\omega'$,如果 $\omega R_{s(i)}^{s(\tau)}\omega'$,则 $\omega_{s(i)}^{s(\tau)}={\omega'}_{s(i)}^{s(\tau)}$,即 $(q_{s(i)}^{\overline{s}(\tau_0)}(\omega),\sigma_{s(i)}^{s(\tau)}(\omega))=(q_{s(i)}^{\overline{s}(\tau_0)}(\omega'),\sigma_{s(i)}^{s(\tau)}(\omega'))$,从而有 $\sigma_{s(i)}^{s(\tau)}(\omega)=\sigma_{s(i)}^{s(\tau)}(\omega')$.由定义 19 知 $\alpha_{s(i)}^{s(\tau)}(\omega)=\alpha_{s(i)}^{s(\tau)}(\omega')$,由定义 25(5)知$\vDash_{\mathcal{M}}^{\omega'}S(i,\tau,m)$.由于$\omega$具有任意性,因此 $B_{i,\tau}S(i,\tau,m)$成立,公理 A11(b)有效.

A11(c). $R(i,\tau,m)\rightarrow B_{i,\tau}R(i,\tau,m)$的有效性可用类似于 A11(b)的方法证明,不同的是所涉及的行为为 $receive(m)$.

A11(d). $H(i,\tau,m)\rightarrow B_{i,\tau}H(i,\tau,m)$.

假设$\vDash_{\mathcal{M}}^{\omega}H(i,\tau,m)$,即 $\overline{s}(m)\in construct_{K_{\overline{s}(i)}^{\overline{s}(\tau)}(\omega)}M_{\overline{s}(i)}^{\overline{s}(\tau)}(\omega)$,则对任意$\omega'$,如果 $\omega R_{\overline{s}(i)}^{\overline{s}(\tau)}\omega'$,则 $\omega_{\overline{s}(i)}^{\overline{s}(\tau)}={\omega'}_{\overline{s}(i)}^{\overline{s}(\tau)}$,即

$$(q_{\overline{s}(i)}^{\overline{s}(\tau_0)}(\omega),\sigma_{\overline{s}(i)}^{\overline{s}(\tau)}(\omega))=(q_{\overline{s}(i)}^{\overline{s}(\tau_0)}(\omega'),\sigma_{\overline{s}(i)}^{\overline{s}(\tau)}(\omega')).$$

由定义 14 有 $\overline{\delta}(q_{\overline{s}(i)}^{\overline{s}(\tau_0)}(\omega),\sigma_{\overline{s}(i)}^{\overline{s}(\tau)}(\omega))=\overline{\delta}(q_{\overline{s}(i)}^{\overline{s}(\tau_0)}(\omega'),\sigma_{\overline{s}(i)}^{\overline{s}(\tau)}(\omega'))$,即$q_{\overline{s}(i)}^{\overline{s}(\tau)}(\omega)=q_{\overline{s}(i)}^{\overline{s}(\tau)}(\omega')$,从而有 $M_{\overline{s}(i)}^{\overline{s}(\tau)}(\omega)=M_{\overline{s}(i)}^{\overline{s}(\tau)}(\omega')$,$K_{\overline{s}(i)}^{\overline{s}(\tau)}(\omega)=K_{\overline{s}(i)}^{\overline{s}(\tau)}(\omega')$.因此,$\overline{s}(m)\in construct_{K_{\overline{s}(i)}^{\overline{s}(\tau)}(\omega')}M_{\overline{s}(i)}^{\overline{s}(\tau)}(\omega')$.由定义 25(4)知,$\vDash_{\mathcal{M}}^{\omega'}H(i,\tau,m)$.由于$\omega'$具有任意性,且 $\omega R_{\overline{s}(i)}^{\overline{s}(\tau)}\omega'$,因此由定义 25(12)可知,$B_{i,\tau}H(i,\tau,m)$成立,该公理有效.

除以上公理外,TCPL 的公理还包括所有以上公理的全称化.以时间变量全称化为例,设$\varphi(\tau)$为 TCPL 的公理,则$\forall_{\tau}\tau\varphi(\tau)$为 TCPL 的公理,以下对其有效性进行证明.

由$\varphi(\tau)$的有效性可知,对任一可能世界$\omega\in W$ 有$\vDash_{\mathcal{M}}^{\omega}\varphi(\tau)$.设 $I(\varphi(\tau))=\overline{\varphi}(s(\tau))$,则在$\omega$中,对任意一种赋值 $s(\tau)$均有 $\overline{\varphi}(s(\tau))$ 成立,即$\vDash_{\mathcal{M}}^{\omega}\varphi[s(\tau)]$.由定义 25(11)知$\vDash_{\mathcal{M}}^{\omega}\forall_{\tau}\tau\varphi(\tau)$,从而$\forall_{\tau}\tau\varphi(\tau)$有效.其他类型变量的全称化可作类似证明. □

定理 14. TCPL 的推理规则(IR)是保持有效的,即如果推理规则的前提有效,则其结论也是有效的.

证明:以下分别证明两条推理规则:

IR(a). $\dfrac{\varphi\rightarrow\psi,\varphi}{\psi}$.

假设$\vDash_{\mathcal{M}}^{\omega}(\varphi\rightarrow\psi)$且$\vDash_{\mathcal{M}}^{\omega}\varphi$,由定义 25(10)知$\nvDash_{\mathcal{M}}^{\omega}\varphi$或$\vDash_{\mathcal{M}}^{\omega}\psi$,且$\vDash_{\mathcal{M}}^{\omega}\varphi$,因此$\vDash_{\mathcal{M}}^{\omega}\psi$ 成立.

IR(b). $\dfrac{\vdash\varphi}{\vdash B_{i,\tau}\varphi}$.

设$\vdash\varphi$,对φ的证明序列的长度n进行归纳.

当n=1时,即φ为公理时,由定理13可知,$\models\varphi$.即对对任意可能世界$\omega\in W$有$\models^{\omega}_{\mathfrak{M}}\varphi$.从而,对任意$i\in A,\tau\in T$,任意可能世界$\omega'\in W$使得$\omega R^{\tau}_{i}\omega'$,有$\models^{\omega}_{\mathfrak{M}}\varphi$.根据定义25(12)有$\models^{\omega}_{\mathfrak{M}}B_{i,\tau}\varphi$,因此$\models B_{i,\tau}\varphi$.

设$n\leqslant k$时有$\models B_{i,\tau}\varphi$,当$n=k+1$时,如果$\varphi$为公理,由上述证明知$\models B_{i,\tau}\varphi$;如果$\varphi$由$\psi,\psi\rightarrow\varphi$经推理规则IR(a)而得到,那么由归纳假设有$\models B_{i,\tau}\psi,\models B_{i,\tau}(\psi\rightarrow\varphi)$,根据A11(a)的有效性知,$\models B_{i,\tau}\varphi$. □

定理15. TCPL的可靠性(soundness)定理:

(1) 对任一TCPL的公式φ,如果$\vdash\varphi$,则$\models\varphi$;

(2) 对任一TCPL的公式φ,如果$\Gamma\vdash\varphi$,则$\Gamma\models\varphi$.

证明:由于情况(1)是情况(2)当Γ为空时的特殊情况,因此,以下只对情况(2)进行证明:

如果$\Gamma\vdash\varphi$,则由定义31可知,存在公式序列$\varphi_1\varphi_2\ldots\varphi_i\ldots\varphi_n$使得$\varphi_n=\varphi$,且$\varphi_i(1\leqslant i\leqslant n)$或者是$\Gamma$中的公式,或者TCPL的公理,或者是由$\varphi_j,\varphi_k(j<i,k<i)$通过TCPL的推理规则得出.以下对该公式序列长度$n$施归纳法进行证明:

归纳基础:当n=1时,φ只可能为公理或Γ中的公式.由定理13知:当φ为公理时,φ是有效的,所以有$\Gamma\models\varphi$;当φ为Γ中的公式时,由定义29可知$\Gamma\models\varphi$.

归纳步骤:假设$n\leqslant k$时命题成立,当$n=k+1$时,如果φ为公理或Γ中的公式,由上述证明知$\Gamma\models\varphi$;如果φ由$\varphi_i,\varphi_j$$(i,j\leqslant k)$经推理规则IR而得到,那么因为$i,j\leqslant k$,根据归纳假设有$\Gamma\models\varphi_i,\Gamma\models\varphi_j$.由定理14可知,如果前提$\Gamma$中的公式均有效则$\varphi$有效,即$\Gamma\models\varphi$.

综合以上可知,TCPL是可靠的(sound). □

雷新锋(1973－),男,陕西洛南人,博士,主要研究领域为信息安全,形式化方法.

肖军模(1947－),男,教授,博士生导师,主要研究领域为信息安全,软件工程.

刘军(1969－),男,副教授,主要研究领域为信息安全,软件工程.