逻辑学研究　2026 年第 1 期，62–88
文章编号：1674-3202(2026)-01-0062-27

独知逻辑与秘密逻辑

熊作军

摘　要：“独知”即仅为某一个体所知，它是该个体秘密地知道（某一命题）的必要条件。本文在知识逻辑的基础上讨论了“独知”模态及其公理系统，并进一步对秘密逻辑系统进行了扩展，构造了基于 **S5** 系统的独知逻辑与 **S4** 系统的纯秘密逻辑。在独知逻辑方面，揭示了其在“无穷主体集”下的非紧致性，并给出了可靠且强完全的“无穷证明系统”。在秘密逻辑方面，对单主体的纯秘密逻辑系统（不含知道算子）**ICST** 进行了扩展，引入了正自省公理（4 公理），得到了 **ICST4** 系统，并通过标准模型与翻译证明了其在自反传递的克里普克模型上的完全性问题。最后，本文对独知逻辑与秘密逻辑的相关研究方向进行了讨论。

关键词：独知；秘密；**ICST4**；无穷证明系统

中图分类号：B81　　**文献标识码：**A

1　引言

自己“独知”（exclusive knowing）即仅为自己所知，自己的秘密（secret）则是自己知道自己独知的信息。秘密信息包含于独知信息之中，知道某信息为自己独知时，则该信息就成为了自己的秘密。在社会生活中，“个人隐私”、“商业机密”等都可以看作是特定个体或群体的秘密信息，对独知逻辑与秘密逻辑的研究，有助于我们把握与理解“隐私”、“机密”等在交流互动中呈现出的逻辑规律。国内外学者对涉及“秘密”这一概念的逻辑研究主要分为两类。一类是将（类似于）“秘密”的概念作为逻辑系统的原子命题（atoms）或概念展开的研究，另一类是将“秘密”作为逻辑语言中的模态算子进行的研究。

在“秘密”作为原子命题或概念使用的研究中，主要有如下这些工作。比如 H. van Ditmarsch 等讨论了关于“流言”（gossip）的逻辑研究，具体分析讨论了流言或秘密等原子命题在不同的传播协议（protocol）下所具有的逻辑特征。（[14]）S. M.

收稿日期：2025-06-12

作者信息：熊作军　西南大学逻辑与智能研究中心
zuojunxiong@swu.edu.cn

基金项目：国家社会科学基金项目“秘密信息的动态认知逻辑研究”（24BZX112）。

致　谢：本文关于 **ICST4** 的部分受益于第 16 届全国现代逻辑学术研讨会匿名评审的建议与会议中的报告交流。

More 和 P. Naumov 则是对作为原子命题的秘密在不同的网络结构中的独立性问题做了探讨。([9, 10]) J. Fan 等从认知逻辑的角度，分析讨论了不同的认知情境，尤其是关于认知模糊性的讨论也涉及到了“知”(knowledge) 与“未知”(ignorance) 间的相互关系，以及由此推导出的主体间的认知互动问题，但并未确切地谈论具有秘密特征的“知识”所呈现的逻辑特性。([7]) 李延军则是从动态逻辑 (Dynamic Logic) 的角度讨论了一种相对于公开宣告而言的“秘密宣告”，将秘密看做一种宣告动作的特点，着重讨论的是在秘密宣告下群体信念状态的变化问题等。([17])

对于“秘密”作为模态算子的逻辑研究正逐渐受到关注。张玉志在其博士论文 ([19]) 中给出了能表达“秘密信息”的一种特殊的模态算子 (S)，但这一算子在逻辑形式上是不能叠加的，因而不能谈论“某人的秘密”这一个命题是否是他人的秘密的问题，并且由于这一秘密算子 S 只是定义在认知逻辑 (Epistemic Logic) ([5]) 中的“知道算子 K”上的，因而未能展示出“秘密”所特有的 (不为知识或信念所具有的) 逻辑特性。进一步，熊作军与张玉志从模态逻辑 (Modal Logic) 的语义角度分析探讨了秘密与知识 (knowledge)、信念 (belief) 之间所具有的相互关系。([18]) 如秘密具有认知逻辑中定义的“真值性” (truth) 与“正自省性” (positive introspection)，但不具有“负自省性” (negative introspection)，并其给出了关于“秘密逻辑”的公理化系统的猜想。熊作军和张玉志介绍了认知逻辑视域下秘密知识 (secret knowledge) 的逻辑分析，其将秘密知识解释为一种“只为自己所知，且自己知道别人不知”的信息。([18]) 比如，称命题 φ 为 a 的秘密，即指“a 知道 φ，且 a 知道其他主体都不知道 φ”。[1] Z. Xiong 和 T. Ågotnes 则进一步给出了极小秘密知识逻辑系统 **ICS** 与自反的秘密知识逻辑系统 **ICST** 的完全性。([16]) A. Aldini 等则使用“知识 (K)、信念 (B) 以及意向 (I)”等模态算子从“主体 a 有意对主体 b 掩藏信息 φ” ($S_{a,b}\varphi$) 的角度讨论了“保密推理”，通过分别给出这三类模态算子的关系语义解释构建了其逻辑模型，讨论了相关推理规则与公理，但这一语言主要围绕“意向”来定义秘密，且缺乏公理系统完全性的证明。([2])

本文基于对张玉志 ([19])、熊作军和张玉志 ([18]) 以及 Z. Xiong 和 T. Ågotnes ([16]) 中秘密逻辑的讨论，在第 2 节进一步审视秘密模态的语义，指出秘密信息中不同层级的理解，由此提炼出“独知”模态，以便更细致地刻画“秘密”。据此，文章将给出“独知逻辑” (Exclusive Knowing Logic) 的模型与公理系统 **S5O**，揭示其在“无穷主体集”下的非紧致性，并给出了其在无穷证明系统上的强完全性。为了探求纯秘密逻辑系统的扩展问题，在第 3 节对 Z. Xiong 和 T. Ågotnes ([16]) 中介绍的单主体视角下纯秘密逻辑 (不含知道算子) 系统进行了扩展，证明 **ICST4** 的完全性问题。最后在第 4 节进行了总结，对独知逻辑与秘密逻辑的相关扩展进行了讨论。

[1] 张玉志则将命题 φ 为 a 的秘密解释为“a 知道 φ，且其他主体都不知道 φ”。([19])

2 “独知”的逻辑系统

[16, 18, 19] 中的秘密逻辑分析的带有秘密信息的命题都是不含主体信息，或者说主体信息是认知主体本身的命题。如“小王的银行卡密码是 1234”、“百元人民币上印有一只猫”都是小王的秘密等。考虑这样一个情形（假设小张知道小王只有一张银行卡）：

例 1 (银行卡密码)**.** 小王在自动取款机上设置银行卡密码，只有小张站在小王身后，他看见了小王设置的密码为 1234，但小王并不知道小张看见了自己设置的密码。

在已有的秘密逻辑中，我们可以从上述例子中得到“小王的银行卡密码是 1234”既不是小张的秘密（因为小王知道这个命题），也不是小王的秘密（因为小张知道这个命题）。但“小张知道小王的银行卡密码是 1234”是小张的秘密，因为这一命题并不为他人所知（小王并不知道小张知道自己的银行卡密码是 1234，且没有其他人知道）。因而，虽然不能在“原子命题”层面上说“小王的银行卡密码是 1234”是小张的秘密，但是可以在“认知命题”层面上说“小张知道小王的银行卡密码是 1234”是小张的秘密。这一点也很好地反映了“小张知道 p”是小张的秘密，并不意味着“p 是小张的秘密”为真，即 $S_aK_a\varphi \to S_a\varphi$ 不是有效式，但纯秘密逻辑系统并不能区分“命题本身的秘密”与“关于命题认知的秘密”。

重新审视“秘密信息”模态的语义定义，在自然语言上“主体 a 秘密地知道命题 φ”至少有两种理解：

1. $S_a\varphi$：命题 φ 为主体 a 所知，且他知道其他人都不知道命题 φ（即 a 独知 φ 且知道自己独知 φ）；
2. $S_aK_a\varphi$：命题 $K_a\varphi$ 为主体 a 所知，且他知道其他人都不知道 $K_a\varphi$（但其他人可能知道命题 φ）。

而 [16, 18] 中将“主体 a 秘密地知道命题 φ”定义为

$$K_a\varphi \wedge K_a \bigwedge_{b\neq a} \neg K_b\varphi \tag{1}$$

其对应的是第 1 种理解。第 2 种理解与第 1 种的不同之处在于只要求其他人不知道 $K_a\varphi$，而非 φ。这意味着，秘密模态可以看成是内嵌“独知”模态的复合模态。“独知信息”是“秘密信息”的必要条件，引入“独知”模态，有助于区分与表达“φ 是 a 的秘密”与“a 秘密地知道 φ”这两种不同层级的秘密概念。据此，我们以知识逻辑的语义为基础，给出一个新的模态公式 $O_a\varphi$（只有主体 a 知道命题 φ）的解释如下：[2]

$$K_a\varphi \wedge \bigwedge_{b\neq a} \neg K_b\varphi \tag{2}$$

[2]该形式定义在 φ 为布尔命题时即是 [19] 中对秘密的解释，即该文献中介绍的“秘密”模态实际上是“独知”模态。

(2)式与秘密的定义（(1)式）的唯一区别在于我们删掉了第二个 K_a 算子。即 $O_a\varphi$ 为真，并不意味着主体 a 知道其他人不知道命题 φ，仅仅是描述命题 φ 为主体 a 所“独知”。而主体 a 秘密地知道命题 φ 的两种不同解释就可分别表达为 $S_a\varphi$ 与 $K_aO_a\varphi$ 逻辑等价，或 $S_aK_a\varphi$ 与 $K_aO_aK_a\varphi$ 逻辑等价。比如用 p 表示“百元人民币上印有一只猫”，K_aO_ap 则表示主体 a 知道只有自己知道“百元人民币上印有一只猫”而别人都不知道这个命题，故 p 是主体 a 的秘密。而 $K_aO_aK_ap$ 则表示主体 a 知道只有自己知道“百元人民币上印有一只猫”而别人都不知道主体 a 知道这个命题，故 K_ap 是主体 a 的秘密（p 并不一定是主体 a 的秘密，完全可以有其他人也知道 p）。

2.1　语言与语义

为了更好地表达出这种秘密信息的不同层次，我们使用独知模态对知识逻辑的语言扩展如下。给定非空原子命题字母集 Prop 与非空主体集 Agt，独知逻辑的公式 $\varphi \in \mathcal{L}_{KO}$ 定义如下：

$$\varphi ::= p \mid \neg\varphi \mid (\varphi \wedge \varphi) \mid K_a\varphi \mid O_a\varphi$$

其中 $p \in$ Prop 为原子命题，$a \in$ Agt 为主体。$K_a\varphi$ 表示主体 a 知道 φ，而 $O_a\varphi$ 表示“只有主体 a 知道 φ”。进一步，$S_a\varphi$ 则是对 $K_aO_a\varphi$ 的简写。[3] 当 $a \neq b$ 时，根据知识模态的自反性，“主体 a 知道只有主体 b 知道 φ”这样的语句是恒假的，在模型上即 $K_aO_b\varphi$ 是不可满足的。同理，再接受知道算子具有正自省性时（即 4 公理），$O_aK_b\varphi$ 也是不可满足的，根据 4 公理，从 $K_b\varphi$ 有 $K_bK_b\varphi$，从而不仅仅只有 $K_aK_b\varphi$，故“只有主体 a 知道主体 b 知道 φ”也是恒假的。这一特点也可以看成是对日常生活中使用“秘密”模态的一种规范。

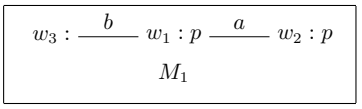
定义 2.1 (语义). 任给 $M = (W, \sim, V)$ 为 **S5** 模型，$\varphi \in \mathcal{L}_{KO}$ 且 $w \in W$。称 φ 在 w 上为真，记作 $M, w \models \varphi$，归纳定义如下：

$M, w \models p$	当且仅当	$w \in V(p)$。
$M, w \models \neg\varphi$	当且仅当	$M, w \not\models \varphi$。
$M, w \models (\varphi \wedge \psi)$	当且仅当	$M, w \models \varphi$ 且 $M, w \models \psi$。
$M, w \models K_a\varphi$	当且仅当	对任意 $u \in W$，$w \sim_a u$ 蕴涵 $M, u \models \varphi$。
$M, w \models O_a\varphi$	当且仅当	对任意 $u \in W$，$w \sim_a u$ 蕴涵 $M, u \models \varphi$ 且 对任意 $b \neq a$ 有 $v \in W$，$w \sim_b v$ 且 $M, v \models \neg\varphi$。

命题 2.1 (独知的意义). 根据独知模态的语义解释，当 $|\text{Agt}| \geq 2$ 时，不难验证如下表达式：

(i) $\models O_a\varphi \to (K_a\varphi \wedge \neg K_b\varphi)$ 其中 $b \neq a$。（“独知不共享”）

[3] 从这个意义上看，多主体秘密逻辑语言是独知逻辑语言的一个子集。



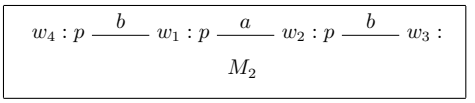


图 1: 模型 M_1 与 M_2，其中 $\sim$ 关系用带标签的线段标注（自反关系省略），可能世界标注在“:”前，原子命题赋值标注在“:”后。

(ii) 从 $\models \varphi$，可知 $\models \neg O_a\varphi$。(“真理不独知”)

命题 2.2 (独知与自省). $\not\models O_a\varphi \to O_aO_a\varphi$；$\not\models \neg O_a\varphi \to O_a\neg O_a\varphi$

证明. 给定 Agt $= \{a, b\}$，令模型 M_1 与 M_2 定义如图1。可知，$M_1, w_2 \models \neg O_a p$，故易见 $M_1, w_1 \models O_a p \wedge \neg O_a O_a p$。而从 $M_2, w_2 \models O_a p$ 易知 $M_2, w_1 \models \neg O_a p \wedge \neg O_a \neg O_a p$。 □

命题 2.3. $\not\models O_a(\varphi \wedge \psi) \to O_a\varphi$。

证明. 给定 Agt $= \{a, b\}$，令 $M = (W, \sim, V)$ 其中 $W = \{w_1, w_2\}$，$\sim_a = \{(w, w) \mid w \in W\}$，$\sim_b = W \times W$ 且 $V(p) = \{w_1, w_2\}$；$V(q) = \{w_1\}$。显然有 $M, w_1 \models O_a(p \wedge q)$ 但 $M, w_1 \models \neg O_a p$。 □

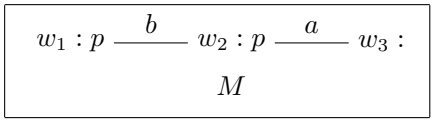
命题 2.4. $\models (O_a\varphi \wedge O_a\psi) \to O_a(\varphi \wedge \psi)$。

证明. 根据语义定义可知。 □

命题 2.5 (独知单调性). $\models O_a\varphi \to O_aK_a\varphi$ 但 $\not\models O_aK_a\varphi \to O_a\varphi$。

证明. 任给点模型 M, w 使得 $M, w \models O_a\varphi$。欲证 $M, w \models O_aK_a\varphi$，先证 (1) 任意 $u \in W$ 若 $w \sim_a u$ 则有 $M, u \models K_a\varphi$。由 $M, w \models O_a\varphi$，据命题2.1(i) 有 $M, w \models K_a\varphi$，再根据 4 公理有 $M, w \models K_aK_a\varphi$，故有 (1) 得证。再证 (2) 对任意 $b \neq a$ 有 $w \sim_b v$ 且 $M, v \models \neg K_a\varphi$。任取 $b \neq a$，根据 $M, w \models O_a\varphi$，有 $M, w \models \neg K_b\varphi$，即有 $w \sim_b v$ 使得 $M, v \models \neg\varphi$，故而根据 T 公理的逆定理，有 $M, v \models \neg K_a\varphi$。故 (2) 得证。综合 (1) 与 (2) 可知，$M, w \models O_aK_a\varphi$。

给定 Agt $= \{a, b\}$，令 $M = (W, \sim, V)$ 定义如下图（相关约定如图1）。



从 $M, w_1 \models K_a p \wedge K_b p$ 可知 $M, w_1 \models \neg O_a p$。但从 $M, w_2 \models \neg K_a p$，$M, w_1 \models K_a p$ 与 $w_1 \sim_b w_2$ 可知 $M, w_1 \models O_aK_a p$。故有 $\not\models O_aK_a\varphi \to O_a\varphi$。 □

利用 K_a 算子的分配性，则有如下关于秘密信息的推论。

推论 1 (秘密的层级). $\models K_aO_a\varphi \to K_aO_aK_a\varphi$（命题信息秘密是知识信息秘密）。[4]

当 Agt $= \{a_1, \cdots, a_n\}$ 为基数大于 1 的有穷主体集时，独知模态可以由如下公式定义：

$$O_a\varphi \leftrightarrow (K_a\varphi \wedge \bigwedge_{b\neq a\in \text{Agt}} \neg K_b\varphi) \tag{3}$$

公式(3)可看成是独知算子 O 对知识算子 K 的归约，称作 O 公理（其可靠性可由语义定义直接推出）。则有 **S5** + O 为基于 **S5** 知识逻辑的独知逻辑公理系统（在 **S5** 系统中添加归约公理 O）。[5] 但当 Agt 为无穷集时，则独知逻辑不具有紧致性。

命题 2.6 (非紧致性). 给定 Agt 为无穷集。则独知逻辑语言是不紧致的。

证明. 令 $\Delta = \{\neg O_ap, K_ap\} \cup \{\neg K_bp \mid b \in \text{Agt}, b \neq a\}$，易见 $\Delta \nvdash \bot$ 但 Δ 是不可满足的；换言之，任意 Δ 的有穷子集是可满足的，但 Δ 本身不可满足。 □

由此可知，给定 Agt 为无穷集时，在有穷证明系统中，独知逻辑是没有强完全性的。类似地，在有穷证明系统中，当 Agt 为无穷集合时，由独知逻辑定义的秘密逻辑也是非紧致的，因而也不具有强完全性。如 $\Delta = \{\neg S_ap, K_ap\} \cup \{K_a\neg K_bp \mid b \in \text{Agt}, b \neq a\}$ 时，可知 Δ 是一致的，但不可满足。

在基本知识逻辑如 **S5** 逻辑中，主体集 Agt 不影响其公理系统。在实际应用中，主体集 Agt 往往都是有穷集，因而讨论“独知”只需要运用“知识逻辑”即可。但我们已经看到，当讨论的主体集 Agt 为无穷集时，独知逻辑是不能化归为知识逻辑的，其公理系统需要进一步研究。我们将在下文中构造可靠且**强完全**的无穷公理系统。

2.2　无穷公理系统

独知逻辑的无穷公理系统 **S5O** 与 [15] 中的公理系统的定义思路类似，详细定义见图 2 ,但我们省略其涉及的“必然形式”（necessity form）。[6] K公理 $K_a(\varphi \to \psi) \to (K_a\varphi \to K_a\psi)$ 可以由图 2 中Nk、MP和导出规则DT推出。**S5O** 可靠性与完全性定义如常：任给 $\mathcal{L}_{KO}$ 的公式集 Γ 与公式 φ，**S5O** 是可靠的即指：从 $\Gamma \vdash_\omega \varphi$，有 $\Gamma \models \varphi$；其（强）完全性则是指：从 $\Gamma \models \varphi$ 可推出 $\Gamma \vdash_\omega \varphi$。值得注意的是，我们对 MP 规则做了适当增强以便在后续证明中使用。无穷规则DeR的自然直观是当

[4] a 知道 φ 是自己的秘密，则 a 也知道 $K_a\varphi$ 是自己的秘密；反之则不成立。

[5] 由此可知，当主体集为大于 1 的有穷集时，知识逻辑与独知逻辑有着相同的表达力。

[6] 因 [15] 中的语言包含动态算子，其涉及无穷前提的 DiA 规则需要加强以保证在“必然形式”中每一处的出现都可以进行代入。在随机公开宣告逻辑（APAL）中也有“必然形式”的设定，参见 [3]。而本文这里是静态语言，类似于“必然形式”上的代入仅涉及“蕴含式的后件”与“K”模态引导的公式，是可由DeR规则、Rt规则与T公理在系统中推导的。

(PC)	所有命题逻辑重言式例示
(T)	$K_a\varphi \to \varphi$
(4)	$K_a\varphi \to K_aK_a\varphi$
(5)	$\neg K_a\varphi \to K_a\neg K_a\varphi$
(Od)	$O_a\varphi \to (K_a\varphi \wedge \neg K_b\varphi)$

(Ax)	$\vdash_\omega \varphi$ 其中 φ 是左侧的公理
(DeR)	$\{\neg K_b\varphi \mid b \in \text{Agt}, b \neq a\} \vdash_\omega K_a\varphi \to O_a\varphi$
(MP)	$\{\varphi, \varphi \to \psi\} \vdash_\omega \psi$
(Nk)	从 $\Gamma \vdash_\omega \varphi$ 推出 $K_a\Gamma \vdash_\omega K_a\varphi$
(W)	从 $\Gamma \vdash_\omega \varphi$ 推出 $\Gamma \cup \Delta \vdash_\omega \varphi$
(Cut)	从 $\Gamma \vdash_\omega \Delta$ 与 $\Gamma \cup \Delta \vdash_\omega \varphi$ 推出 $\Gamma \vdash_\omega \varphi$

图 2: 独知逻辑的无穷公理系统 **S5O**，$\vdash_\omega$ 是对 $\vdash_{\omega\ \mathbf{S5O}}$ 的简写，其中 $\vdash_\omega \varphi$ 是 $\varnothing \vdash_\omega \varphi$ 的简写，$K_a\Gamma = \{K_a\psi \mid \psi \in \Gamma\}$，当 $\Gamma = \varnothing$ 时，$K_a\Gamma = \varnothing$。$\Gamma \vdash_\omega \Delta$ 是指 Γ 可推出 Δ 中的所有公式，即对任意的 $\delta \in \Delta$，有 $\Gamma \vdash_\omega \delta$。

我们有 $\neg K_b\varphi$ 这一表达式对任意 $b \neq a$ 都成立时，可推出 $K_a\varphi \to O_a\varphi$ 也成立，其可靠性由“独知”的语义解释保证，其余公理与规则的可靠性是显然的。

独知逻辑典范模型定义与基本模态逻辑的类似（[11]，第 4 章），为了后续证明自洽，定义如下。

定义 2.2 (典范模型)**.** 称 $M^c = (W^c, \sim^c, V^c)$ 是独知逻辑的典范模型，即指：

- W^c 是所有极大 $\vdash_\omega$ 一致集的集合。
- 对任意的 $a \in \text{Agt}$ 任给 $\Delta, \Gamma \in W^c$，有 $\Delta \sim_a^c \Gamma$ 当且仅当对任意的 $K_a\varphi \in \Delta$，有 $\varphi \in \Gamma$。
- 对任意的 $p \in \text{Prop}$，任意的 $\Delta \in W^c$：$\Delta \in V^c(p)$ 当且仅当 $p \in \Delta$。

下列命题是我们证明存在引理（引理 2.3 ）的关键。

命题 2.7. *任给集合 Δ 以及 $a \in \text{Agt}$，若 $\{\psi \mid K_a\psi \in \Delta\} \vdash_\omega \varphi$，则 $\Delta \vdash_\omega K_a\varphi$。*

证明. 令 $\{\psi \mid K_a\psi \in \Delta\} \vdash_\omega \varphi$，根据 Nk，有：

$$K_a\{\psi \mid K_a\psi \in \Delta\} \vdash_\omega K_a\varphi$$

根据定义，由于 $K_a\{\psi \mid K_a\psi \in \Delta\} = \{K_a\psi \mid K_a\psi \in \Delta\} \subseteq \Delta$，重复使用 Mo，则有 $\Delta \vdash_\omega K_a\{\psi \mid K_a\psi \in \Delta\}$。最后根据 W、Cut，可得 $\Delta \vdash_\omega K_a\varphi$。 □

为了进一步简化证明，我们使用到了图 3 中的导出规则，具体的推导过程可参见 [15]，引理 10。

引理 2.1 (导出规则)**.** *图3中的所有表达式都成立。*

至此，我们可以证明独知逻辑的 Lindenbaum 引理，其证明策略与 [15, 引理 12] 中的一样，但由于无穷规则的不同，具体证明细节是不同的。该证明的简要思路是通过保证每一DeR-式都包含有“见证”公式来构造一致集，然后通过证明

(Mo)	$\Gamma \cup \{\varphi\} \vdash_\omega \varphi$
(Imp)	从 $\Gamma \vdash_\omega \varphi$ 和 $\Gamma \vdash_\omega \varphi \to \psi$，推出 $\Gamma \vdash_\omega \psi$
(Rt)	从 $\Gamma \vdash_\omega \varphi \to \psi$ 推出 $\Gamma \cup \{\varphi\} \vdash_\omega \psi$
(DT)	从 $\Gamma \cup \{\varphi\} \vdash_\omega \psi$ 推出 $\Gamma \vdash_\omega \varphi \to \psi$
(Raa)	从 $\Gamma \cup \{\varphi\} \vdash_\omega \bot$ 推出 $\Gamma \vdash_\omega \neg\varphi$
(Con)	从 $\Gamma \vdash_\omega \varphi \wedge \psi$ 推出 $\Gamma \vdash_\omega \varphi$ 和 $\Gamma \vdash_\omega \psi$

图 3: 独知逻辑的无穷公理系统 **S5O** 的部分导出规则。

“无穷证明的单调闭包性”（见(4)）来完成从“任意 Γ_i 是一致的”向“$\bigcup_{i\in\mathbb{N}}\Gamma_i$ 也一致”的证明。

引理 2.2 (Lindenbaum 引理)**.** *任给一个独知逻辑的一致公式集 Γ，存在一个极大一致的公式集 Γ' 使得 $\Gamma \subseteq \Gamma'$。*

证明. 回顾DeR规则，使用Rt规则可转化为DeR变形规则：$\{\neg K_b\varphi \mid b \in \text{Agt}, b \neq a\} \cup \{K_a\varphi\} \vdash_\omega O_a\varphi$。称形如 $O_a\varphi$ 的公式为 **DeR-式**，而 $(K_a\varphi \wedge \neg K_b\varphi)$ 则为 **DeR-见证**。给定 Γ 为一致的公式集以及 $\psi_1, \psi_2, \cdots$ 为独知逻辑 $\mathcal{L}_{KO}$ 所有公式的一个序列。$\Gamma' \supseteq \Gamma$ 归纳定义如下：

- $\Gamma_0 = \Gamma$
- $\Gamma_{i+1} = \begin{cases} \Gamma_i \cup \{\psi_{i+1}\} & \text{若 } \Gamma_i \vdash_\omega \psi_{i+1} \\ \Gamma_i \cup \{\neg\psi_{i+1}\} & \text{若 } \Gamma_i \nvdash_\omega \psi_{i+1} \text{ 且 } \psi_{i+1} \text{ 不是DeR-式} \\ \Gamma_i \cup \{\neg\psi_{i+1}, \neg\psi_{i+1}(b)\} & \text{若 } \Gamma_i \nvdash_\omega \psi_{i+1} \text{ 且 } \psi_{i+1} = O_a\varphi, \\ & \psi_{i+1}(b) = K_a\varphi \wedge \neg K_b\varphi \text{ 且 } \Gamma_i \nvdash_\omega \psi_{i+1}(b), b \neq a \in \text{Agt} \end{cases}$
- $\Gamma' = \bigcup_{i\in\mathbb{N}}\Gamma_i$

Γ' 的极大性可从其构造中得出；对于 ψ_{i+1} 是形如DeR-式的 $O_a\varphi$ 时，我们可以通过DeR规则保证至少有一个 $b \neq a$ 的DeR-见证使得 $\Gamma_i \nvdash_\omega K_a\varphi \wedge \neg K_b\varphi$，否则有 $\Gamma_i \vdash_\omega \psi_{i+1}$，与扩张条件矛盾。现在，我们证明 Γ_i 是 $\vdash_\omega$ 一致的。施归纳于 i。根据前提，$\Gamma_0 = \Gamma$ 是一致的。假设 Γ_j 是一致的，现证明 Γ_{j+1} 也是一致的。考虑其生成的三种情况：（C1）当 $\Gamma_{j+1} = \Gamma_j \cup \{\psi_{j+1}\}$ 时，根据其生成条件，显然其是一致的。（C2）当 $\Gamma_{j+1} = \Gamma_j \cup \{\neg\psi_{j+1}\}$ 时，若 $\Gamma_j \cup \{\neg\psi_{j+1}\} \vdash_\omega \bot$，则根据Raa规则有 $\Gamma_j \vdash_\omega \psi_{j+1}$，与条件矛盾。（C3）当 $\Gamma_{j+1} = \Gamma_j \cup \{\neg\psi_{j+1}, \neg\psi_{j+1}(b)\}$ 其中 ψ_{j+1} 是DeR-式的 $O_a\varphi$ 且有 $b \neq a$ 使得 $\psi_{j+1}(b) = K_a\varphi \wedge \neg K_b\varphi$ 是其DeR-见证。假设 $\Gamma_j \cup \{\neg\psi_{j+1}, \neg\psi_{j+1}(b)\} \vdash_\omega \bot$，据Raa规则有 (i) $\Gamma_j \cup \{\neg\psi_{j+1}(b)\} \vdash_\omega \psi_{j+1}$，即 $\Gamma_j \cup \{\neg\psi_{j+1}(b)\} \vdash_\omega O_a\varphi$，再根据W规则与 Od 公理，有 $\Gamma_j \cup \{\neg\psi_{j+1}(b)\} \vdash_\omega O_a\varphi \to (K_a\varphi \wedge \neg K_b\varphi)$，即有 (ii)$\Gamma_j \cup \{\neg\psi_{j+1}(b)\} \vdash_\omega \psi_{j+1} \to \psi_{j+1}(b)$，再根据MT有 (ii) $\Gamma_j \cup \{\psi_{j+1}, \neg\psi_{j+1}(b)\} \vdash_\omega \psi_{j+1}(b)$，再根据 (i) 使用Cut规则，有 $\Gamma_j \cup \{\neg\psi_{j+1}(b)\} \vdash_\omega \psi_{j+1}(b)$。

根据DT规则有 $\Gamma_j \vdash_\omega \neg\psi_{j+1}(b) \to \psi_{j+1}(b)$。再根据Ax公理中的命题逻辑公理和W规则，有 $\Gamma_j \vdash_\omega (\neg\psi_{j+1}(b) \to \psi_{j+1}(b)) \to \psi_{j+i}(b)$。再根据Imp规则有 $\Gamma_j \vdash_\omega \psi_{j+1}(b)$ 与条件中的 $\Gamma_j \not\vdash_\omega \psi_{j+1}(b)$ 矛盾。综合三种情况，得证 Γ_j 是一致的，即对任意 $i \in \mathbb{N}$：Γ_i 都是一致的。欲证 Γ' 是一致的，先证明：[7]对任意独知逻辑公式集 Γ'' 与公式 φ 使得 $\Gamma'' \vdash_\omega \varphi$，有

$$\text{若 } \Gamma'' \subseteq \Gamma', \text{ 则 } \varphi \in \Gamma'。 \tag{4}$$

证明思路是对 $\Gamma'' \vdash_\omega \varphi$ 的情况的进行归纳，DeR规则的证明类似于 [15, 引理 12] 中 **DiA** 的证明，其余的则可参见 [1]。从(4)可知，当 $\Gamma'' = \Gamma'$ 以及 $\varphi = \bot$ 时，有 Γ' 是不一致时（$\Gamma' \vdash_\omega \bot$ ）推出 $\bot \in \Gamma'$，根据 Γ' 的构造，即有 $j \in \mathbb{N}$ 使得 $\bot \in \Gamma_j$，这与 Γ_j 是一致的相矛盾。故 Γ' 的一致性得证。综合可知，Γ' 是极大 $\vdash_\omega$ 一致集。 □

引理 2.3 (存在引理). *任给极大 $\vdash_\omega$ 一致集合 Δ，若 $O_a\varphi \in \Delta$，则有*

(C1) *对任意的极大 $\vdash_\omega$ 一致集合 Γ，若 $\Delta \sim_a^c \Gamma$，则 $\varphi \in \Gamma$；且*
(C2) *对任意的 $b \neq a \in$ Agt，存在极大 $\vdash_\omega$ 一致集合 Γ' 使得 $\Delta \sim_b^c \Gamma'$ 且 $\neg\varphi \in \Gamma'$。*

证明. (C1) 可从典范关系 $\sim_a^c$ 的定义与Od公理中得出。现证明 (C2)。任给 $b \neq a \in$ Agt，令 $\Gamma'' = \{\psi \mid K_b\psi \in \Delta\} \cup \{\neg\varphi\}$。先证 Γ'' 的 $\vdash_\omega$ 一致性。使用反证法。若 $\Gamma'' \vdash_\omega \bot$，则根据DT规则，有 $\{\psi \mid K_b\psi \in \Delta\} \vdash_\omega \neg\varphi \to \bot$，据Raa规则，则有 $\{\psi \mid K_b\psi \in \Delta\} \vdash_\omega \neg\neg\varphi$，易得 $\{\psi \mid K_b\psi \in \Delta\} \vdash_\omega \varphi$。根据命题2.7可知（a）$\Delta \vdash_\omega K_b\varphi$。再根据 $\Delta \vdash_\omega O_a\varphi$，$b \neq a$ 以及Od公理和W规则，有 $\Delta \vdash_\omega O_a\varphi \to (K_a\varphi \wedge \neg K_b\varphi)$，据Imp则有 $\Delta \vdash_\omega (K_a\varphi \wedge \neg K_b\varphi)$，根据Con规则，$\Delta \vdash_\omega \neg K_b\varphi$，与（a）知 Δ 是 $\vdash_\omega$ 不一致的，与假设矛盾。故 Γ'' 是 $\vdash_\omega$ 一致的，根据引理2.2，有极大 $\vdash_\omega$ 一致集 Γ' 使得 $\Gamma'' \subseteq \Gamma'$ 且有 $\Delta \sim_c^b \Gamma'$，$\neg\varphi \in \Gamma'$。 □

引理 2.4 (真值引理). *给定独知逻辑的典范模型 M^c，且 Γ 为极大 $\vdash_\omega$ 一致集，$\varphi \in \mathcal{L}_{KO}$ 为任意公式，则有：$M^c, \Gamma \models \varphi$ 当且仅当 $\varphi \in \Gamma$。*

证明. 施归纳于 φ 的结构。φ 为原子公式时，由典范模型的定义易证；φ 为布尔公式时，可通过归纳假设 I.H. 得证；$\varphi = K_a\psi$ 时，证明策略与基本认知逻辑类似。这里仅讨论 $\varphi = O_a\psi$ 的情况。

（$\Rightarrow$）令 $M^c, \Gamma \models O_a\psi$，根据语义定义，对任意极大 $\vdash_\omega$ 一致集 Δ，若 $\Gamma \sim_a^c \Delta$，则 $M^c, \Delta \models \psi$，且对任意 $b \neq a \in$ Agt，有极大 $\vdash_\omega$ 一致集 Ω 使得 $\Gamma \sim_b^c \Omega$ 且 $M^c, \Omega \models \neg\psi$。再根据归纳假设 I.H. 有：对任意极大 $\vdash_\omega$ 一致集 Δ，若 $\Gamma \sim_a^c \Delta$，则 $\psi \in \Delta$，且对任意 $b \neq a \in$ Agt，有极大 $\vdash_\omega$ 一致集 Ω 使得 $\Gamma \sim_b^c \Omega$ 且 $\neg\psi \in \Omega$。根据典范关系定义，则有 $K_a\psi \in \Gamma$ 且对任意 $b \neq a \in$ Agt，有 $\neg K_a\psi \in \Gamma$；故据DeR规则，有 $O_a\psi \in \Gamma$。

[7]无穷证明系统中不能从任意有穷子集一致推得集合本身一致，故需要新方法以证明集合本身的一致性。

（⇐）令 $O_a\psi \in \Gamma$，根据典范关系定义与引理2.3有：对任意极大 $\vdash_\omega$ 一致集 Δ，若 $\Gamma \sim_a^c \Delta$，则 $\psi \in \Delta$，且对任意 $b \neq a \in$ Agt，有极大 $\vdash_\omega$ 一致集 Ω 使得 $\Gamma \sim_b^c \Omega$ 且 $\neg\psi \in \Omega$；再据归纳假设 I.H. 有：对任意极大 $\vdash_\omega$ 一致集 Δ，若 $\Gamma \sim_a^c \Delta$，则 $M^c, \Delta \models \psi$，且对任意 $b \neq a \in$ Agt，有极大 $\vdash_\omega$ 一致集 Ω 使得 $\Gamma \sim_b^c \Omega$ 且 $M^c, \Omega \models \neg\psi$；结合语义定义，有 $M^c, \Gamma \models O_a\psi$。 □

定理 2.5 (强完全性)**.** 任给公式集 Γ 与公式 $\varphi \in \mathcal{L}_{KO}$，若 $\Gamma \models \varphi$，则 $\Gamma \vdash_\omega \varphi$。

证明. 证其逆否命题。令 $\Gamma \not\vdash_\omega \varphi$。若 $\Gamma \cup \{\neg\varphi\}$ 是 $\vdash_\omega$ 不一致的，则 $\Gamma \cup \{\neg\varphi\} \vdash_\omega \bot$，据DT规则有 $\Gamma \vdash_\omega \neg\varphi \to \bot$，再根据Ax中的PC公理 $\vdash_\omega (\neg\varphi \to \bot) \to \varphi$、W规则与Imp规则，则有 $\Gamma \vdash_\omega \varphi$，与假设 $\Gamma \not\vdash_\omega \varphi$ 矛盾，故 $\Gamma \cup \{\neg\varphi\}$ 是 $\vdash_\omega$ 一致的。进而根据引理2.2，有极大 $\vdash_\omega$ 一致集 Γ' 使得 $\Gamma \cup \{\neg\varphi\} \subseteq \Gamma'$，从而根据引理2.4和 $\neg\varphi \in \Gamma'$ 有 $M^c, \Gamma' \models \neg\varphi$，即有 $\Gamma' \not\models \varphi$。 □

至此，我们给出了基于知识逻辑的独知逻辑的可靠且完全的无穷公理系统。借助于知识算子与独知算子，我们可以刻画不同层次的秘密命题（φ 是秘密与秘密地知道 φ），这一点为我们谈论秘密提供了新的工具。独知是秘密的必要条件，因而关注“独知”模态有助于系统分析“秘密”模态，但独知逻辑是借助于知道算子来把握秘密信息的，不依赖于知道算子的纯秘密逻辑还可以接受哪些命题？我们将在下一节参照知识公理对纯秘密逻辑展开讨论。

3　“秘密”的逻辑系统

称仅含有“秘密”这一模态算子的逻辑为纯秘密逻辑，本节将在 [16] 介绍的 **ICST** 基础上，完成其对正自省公理（4 公理）扩展的完全性证明。为了自洽，我们将在第 3.1 小节介绍（单主体）秘密逻辑的语言与语义。由于包含知道算子的秘密逻辑在至少包含两个主体的有穷主体集上是可由知道算子定义的，因而我们将秘密逻辑限制为纯秘密逻辑。在第 3.2 小节进一步给出需要提及和使用的 **ICS** 与 **ICST** 系统的定义、定理等，并进一步讨论了相关公理的独立性问题。本节的重点工作集中在第 3.3 小节，我们根据“带标签的极大一致集”先构造保证自反但不保证传递性的“预模型”（pre-model），然后再在预模型上构造真正的“典范标准模型”，这不是 **ICS** 与 **ICST** 系统完全性证明方法的直接套用，其证明方法对类似的标签系统具有一定的启发性。最后，我们在第 3.4 小节对 **ICST4** 系统进行了讨论。

3.1 语言与语义

给定 Prop 为原子命题字母集，Agt 为至少包含两个主体的主体集。秘密逻辑的形式语言 $\varphi \in \mathcal{L}_{SK}$ 是对知识逻辑的扩张，具体定义如下：

$$\varphi ::= p \mid \neg\varphi \mid (\varphi \wedge \varphi) \mid K_a\varphi \mid S_a\varphi$$

其中 $p \in$ Prop，$a \in$ Agt。其余布尔联结词定义如常，$K_a\varphi$ 读作“a 知道 φ”，$S_a\varphi$ 读作“φ 是 a 的秘密”。$K_a\varphi$ 的语义解释见定义2.1，$S_a\varphi$ 的语义解释见定义3.2。$\langle S_a\rangle$ 算子是 S_a 的对偶算子，即 $\neg S_a\neg$ 的简写。需要注意的是，在纯秘密逻辑中，我们的“秘密模型”并不是定义为 **S5** 模型，而只是 **K** 模型。我们是通过添加公理的方式来刻画 **KT**、**S4** 等模型的，在刻画 **S5** 模型方面还有困难，我们将在第3.4小节中讨论。

与在独知逻辑中的讨论类似，当主体集 Agt 为大于 1 的有穷主体集时，$S_a\varphi$ 可由知道算子定义：

$$S_a\varphi \leftrightarrow (K_a\varphi \wedge K_a \bigwedge_{b\neq a} \neg K_b\varphi) \tag{5}$$

因而，在主体集为大于 1 的有穷集时，$\mathcal{L}_{SK}$ 的表达力与基本的知识逻辑表达力相同，其公理系统就是在知识逻辑公理系统上加入公式(5)作为公理。同理，由命题 2.6后的讨论可知，当 Agt 为无穷集时，$\mathcal{L}_{SK}$ 也是不紧致的，因而其没有强完全的有穷公理系统。更多关于知识与秘密的互动、有效式与定理证明参见 [16, 18]。

在主体集 Agt 为无穷集的条件下，我们也可以仿照独知逻辑无穷公理系统（见第 2.2 节）的构建与证明思路，构建（带有知道算子的）秘密逻辑的无穷公理系统。这样的定义与证明在技术上只是繁琐，并不困难，故本文不再进一步展开。相反，我们将回到有穷主体集（双主体集）的设置下，讨论纯秘密逻辑公理系统的正自省性扩展。

令 $\mathcal{L}_S \subseteq \mathcal{L}_{SK}$ 为纯秘密逻辑语言，具体表达如下（相关解释见 $\mathcal{L}_{SK}$）：

$$\varphi ::= p \mid \neg\varphi \mid (\varphi \wedge \varphi) \mid S_a\varphi$$

由于本节主要关注纯秘密逻辑下单主体秘密逻辑的公理系统问题，为了简练，我们与 [16] 保持一致，只讨论关于确定主体 a 的秘密知识问题。[8] 因此，我们在本节中将省略主体词 a，使用 $S\varphi$ 表示公式 $S_a\varphi$，其具体解释见定义3.2，并将所有不同于 a 的主体看成是主体 b，并在这一逻辑中约定 Agt $= \{a, b\}$。

定义 3.1 (秘密模型). 一个秘密模型 $M = (W, R_a, R_b, V)$ 的定义如下：

[8]这里关注单主体的“秘密信息”，一是为了便于系统证明，二是为了探清“单主体视域”下秘密信息呈现的本质特征。显然，在多主体系统下，秘密信息的交互会更加有趣，比如会有“$S_ap \to \neg S_bp$（$a \neq b$）”这样的有效式，详见 [16, 18]。

- W 是非空世界集，指代不同的可能世界（或状态）；
- R_a 与 R_b 是 W 上的二元关系，即 $R_a \subseteq (W \times W)$ 且 $R_b \subseteq (W \times W)$；
- V : Prop $\to \mathcal{P}(W)$ 是原子命题字母集上满足 $V(p) \subseteq W$ 的赋值函数。

若删除赋值函数 V，则称结构 (W, R_a, R_b) 为秘密框架，且也称 (W, R_a, R_b, V) 是由框架 (W, R_a, R_b) 生成的模型。

定义 3.2 (语义解释)**.** 令 $M = (W, R_a, R_b, V)$ 为秘密模型且 $\varphi \in \mathcal{L}_S$ 为秘密逻辑公式。称 φ 在模型 M 的 w 世界上为真，记作：$M, w \models \varphi$，可归纳定义如下：

$M, w \models p$　　当且仅当　$w \in V(p)$。
$M, w \models \neg\psi$　　当且仅当　$M, w \not\models \psi$。
$M, w \models (\psi_1 \wedge \psi_2)$　当且仅当　$M, w \models \psi_1$ 且 $M, w \models \psi_2$。
$M, w \models S\psi$　　当且仅当　对任意 $u \in W$，若 wR_au，则 [$M, u \models \psi$ 且存在 $v \in W$ 使得 uR_bv 且 $M, v \models \neg\psi$]。

$M \models \varphi$ 与 $F \models \varphi$（F 为框架）以及 φ 是有效式（记作 $\models \varphi$）的定义如常。

此外，根据上述秘密模态词 S 的定义，其对偶算子的解释如下：

$M, w \models \langle S\rangle\psi$　当且仅当　存在 $u \in W$ 使得 wR_au 且 [$M, u \models \psi$ 或对任意 $v \in W$，若 uR_bv 则 $M, v \models \neg\psi$]。

与 [16] 一样，为了便于在完全性系统证明中使用典范模型方法，我们使用了其给出的“标准模型”（standard model）语义来构造典范模型。如下简述标准模型的定义及相关定理。

定义 3.3 (标准模型，见 [16])**.** 一个标准模型 $M^o = (W, O, V)$ 的定义如下：

- W 是非空世界集。
- O 是 W 上的满足如下两个条件的三元关系：

  (i) 对任意 $w, u \in W$：$O(w, u, u)$ 当且仅当存在 $v \in W$ 使得 $O(w, u, v)$；
  (ii) 对任意 $w, w', u, v, v' \in W$：若 $O(w, u, v)$ 且 $O(w', u, v')$ 则 $O(w, u, v')$。

- V 是从原子命题字母集 Prop 到 W 幂集的赋值函数。

与秘密框架的定义类似，若去除赋值函数 V，则称 (W, O) 为标准框架。

条件 (i) 对应着在秘密模型中 R_b-自反的不可区分性，而 (ii) 则是对 R_a 与 R_b 关系的复合，它服务于标准模型与其秘密模型间逻辑等价的证明。秘密逻辑语言 $\mathcal{L}_S$ 在标准模型中的解释如下。[9]

[9]为了简化完全性证明，我们使用了 $\langle S\rangle$ 算子来代替 S 算子。

定义 3.4 (标准语义，见 [16]). 对任意的点标准模型 (M^o, w) 以及 $\varphi \in \mathcal{L}_S$，$M^o, w \models \varphi$ 归纳定义如下：

$M^o, w \models p$ 当且仅当 $w \in V(p)$。
$M^o, w \models \neg\varphi$ 当且仅当 $M^o, w \not\models \varphi$。
$M^o, w \models (\varphi \wedge \psi)$ 当且仅当 $M^o, w \models \varphi$ 且 $M^o, w \models \psi$。
$M^o, w \models \langle S\rangle\varphi$ 当且仅当 存在 $u \in W$ 使得 $O(w, u, u)$ 且 $[M^o, u \models \varphi$，或对任意 $v \in W$ 有 $O(w, u, v)$ 蕴涵 $M^o, v \models \neg\varphi]$。

显然，秘密模态 $\langle S\rangle$ 的对偶算子 S 则被解释如下：

$M^o, w \models S\psi$ 当且仅当 对任意 $u \in W$，若 $O(w, u, u)$ 则 $[M^o, u \models \psi$ 且存在 $v \in W$ 使得 $O(w, u, v)$ 且 $M^o, v \models \neg\psi]$。

定义 3.5 (翻译，见 [16]). 给定标准模型 $M^o = (W, O, V)$，其翻译 $Tr(M^o) = (W, R_a, R_b, V)$（即秘密模型）在二元关系 R_a, R_b 上定义如下（W 与 V 保持不变）：wR_au 当且仅当存在 $v \in W$ 使得 $O(w, u, v)$；wR_bu 当且仅当存在 $v \in W$ 使得 $O(v, w, u)$。称 $Tr(M^o)$ 为 M^o 模型的翻译。

根据上述翻译定义，有如下定理：

定理 3.1 (见 [16]). *任给标准模型 M^o。$Tr(M^o)$ 为其翻译模型且满足对任意 $\varphi \in \mathcal{L}_S$：$M^o, w \models \varphi$ 当且仅当 $Tr(M^o), w \models \varphi$。*

定理 3.2 (见 [16]). *任给秘密模型 M，存在一个标准模型 M^o 使得对任意 $\varphi \in \mathcal{L}_S$：$M, w \models \varphi$ 当且仅当 $M^o, w \models \varphi$。*

上述的定理 3.1 与定理 3.2 使得标准模型与秘密模型在我们的秘密逻辑系统下是逻辑等价的，故可在标准模型的语义下来证明秘密逻辑系统的完全性。

3.2 ICS 与 ICST 系统

在证明 **ICST4** 的完全性之前，我们先给出一些必要的定义、定理与解释，并证明 **ICS** 与 **ICST** 系统（见图4）中秘密公理 S 的独立性。从图4可知，秘密公理 S 表达了重言式与矛盾式是等秘的，它与 I 规则（插值规则，Interpolation rule）[10]可以看成是秘密逻辑系统的本质特征。

定义 3.6 (模态关系集，见 [16]). 令 Δ 为极大一致的公式集，并有如下简记：

- $S(\Delta) := \{\varphi \mid S\varphi \in \Delta\}$，

[10]在 [8] 中，这样的规则形式也被称为“凸性”（convexity）规则，这一性质在关于“无知”的逻辑中也有体现，见 [6]。我们倾向于叫它“插值规则”，源自于对“Craig 插值定理”（Craig's Interpolation Theorem）的类似理解，见 [4]，当然，这只是在形式上类似，实质不同，我们对如何称呼这一规则持开放态度。

(PC)	所有命题逻辑重言式例示
(C)	$\vdash (S\varphi \wedge S\psi) \to S(\varphi \wedge \psi)$
(S)	$\vdash S\top \leftrightarrow S\bot$
(T)	$\vdash S\varphi \to \varphi$
(4)	$\vdash S\varphi \to SS\varphi$
(5)	$\vdash \neg S\varphi \to S\neg S\varphi$
(MP)	从$\vdash \varphi \to \psi$ 和$\vdash \varphi$，推出$\vdash \psi$
(I)	从$\vdash \varphi \to \psi$ 和$\vdash \psi \to \chi$，推出$\vdash (S\varphi \wedge S\chi) \to S\psi$

图 4: **ICST5**、**ICST4**、**ICST**、**ICS** 系统（根据是否包含 T、4、5 公理确定，$\vdash$ 则依次被理解为$\vdash_{\mathbf{ICST5}}$、$\vdash_{\mathbf{ICST4}}$、$\vdash_{\mathbf{ICST}}$ 以及$\vdash_{\mathbf{ICS}}$）。

- $N(\Delta) := \{\varphi \mid \langle S\rangle\varphi \in \Delta\}$，
- $E(\Delta) := \{\neg\chi \mid S(\Delta) \vdash \neg\chi, \chi \in N(\Delta)\}$。

再令 $L(\varphi)$ 是包含公式 φ 的极大一致集的集合。

如下关于 Ra/Rab 关系的定义与定义 3.6 一起，可帮助我们表达不同的 a-b 路径与关系，从而有助于构造典范关系。

定义 3.7 (Ra/Rab 关系集，见 [16]). 令 Δ 为极大一致集。若 $S(\Delta)$ 是不一致的，则令 $Ra(\Delta) = \varnothing$；否则，$Ra(\Delta) = \{\Delta' \mid \Delta'$ 是一个极大一致集且 $S(\Delta) \subseteq \Delta'\}$。当 $S(\Delta)$ 是一致集时（否则，则未定义），进一步有如下定义。

- 若 $E(\Delta) \neq \varnothing$，则 $Rab(\Delta) = \{L(\neg\chi) \mid \neg\chi \in E(\Delta)\}$；
- 若 $E(\Delta) = \varnothing$，则 $Rab(\Delta) = \{L(\neg\bot)\}$。[11]

命题 3.1 (秘密内容一致性，见 [16]). 令 Δ 为极大一致集。$S(\Delta)$ 是一致的，当且仅当存在 $\varphi \in \mathcal{L}_S$ 使得 $\varphi \notin S(\Delta)$。

命题 3.2 (秘密见证性，见 [16]). 令 Δ 为极大一致集。若 $S(\Delta)$ 是一致的，则对任意 $\delta \in S(\Delta), \chi \in E(\Delta), \{\neg\delta, \chi\}$ 是一致的。

定理 3.3 (完全性，见 [16]). **ICS** 对于任意克里普克框架类是可靠且强完全的。**ICST** 对于 R_a 与 R_b 自反的克里普克框架类是可靠且强完全的。[12]

下面，我们讨论秘密公理 S 在 **ICST** 系统中的独立性问题。令 **ICT** 是通过删除 **ICST** 中的 S 公理得到的系统，则有如下命题。

[11] 为了简化表达，在后文中，我们用 $\top$ 代替 $\neg\bot$。

[12] 在单主体系统中，主体 b 的认知不可区分关系无法被秘密算子表达，因而 [16] 也证明了 **ICST** 对 R_a 自反的克里普克框架类是可靠且强完全的。

命题 3.3 (ICT 与 ICST). $\vdash_{\mathbf{ICT}} \neg S\bot$ 且 $\vdash_{\mathbf{ICST}} \neg S\top$。

证明. 从 $\vdash_{\mathbf{ICT}} S\bot \to \bot$ 有 $\vdash_{\mathbf{ICT}} \neg S\bot$，故有 $\vdash_{\mathbf{ICST}} \neg S\top$（S 公理）。 □

命题 3.4 ($\nvdash_{\mathbf{ICT}} \neg S\top$). $\neg S\top$ 在 **ICT** 中是不可推导的。

证明.（反证法）假设 $\neg S\top$ 在 **ICT** 下是可推导的，则在其扩张（引入必然化规则 N：从 φ，可推出 $S\varphi$）**ICTN** 下依然可推导。从 $\vdash_{\mathbf{ICTN}} \top$ 根据 N 规则，易证 $\vdash_{\mathbf{ICTN}} S\top$。结合 $\vdash_{\mathbf{ICTN}} \neg S\top$（假设），可知 **ICTN** 是不可靠的。但 **ICTN** $\subset$ **KT** 且 **KT** 是可靠的[13]，故矛盾。 □

此外，S 公理在 **ICST** 下也是独立的（只有 $S\bot \to S\top$ 在 **ICT** 下是可推导的）。从命题 3.3 与命题 3.4 中，易证 $S\top \to S\bot$ 在 **ICT** 下是不可推导的。[14] 再讨论 5 公理：$\neg S\varphi \to S\neg S\varphi$。令 **ST** 为命题逻辑系统引入 S、T 公理以及等值替换规则 RE[15]后的系统。则可证 5 公理在 **ST** 及其扩张下都是不一致的。

命题 3.5 (负自省的脆弱性). 5 公理在 **ST** 下是不一致的。

证明. 令 $\vdash$ 为 $\vdash_{\mathbf{ST}}$。只需证明 $\vdash \neg(\neg S\top \to S\neg S\top)$：

1.	$\vdash S\top \leftrightarrow S\bot$	S	5.	$\vdash S\neg S\top \leftrightarrow S\top$	RE, 4
2.	$\vdash S\bot \to \bot$	T	6.	$\vdash \neg S\neg S\top$	PC, 3 + 5
3.	$\vdash \neg S\top$	PC, 1 + 2	7.	$\vdash \neg S\top \wedge \neg S\neg S\top$	PC, 3 + 6
4.	$\vdash \neg S\top \leftrightarrow \top$	PC, 3	8.	$\vdash \neg(\neg S\top \to S\neg S\top)$	PC, 7

□

此外，[16] 中使用邻域语义（neighbourhood semantics）证明了 I 规则的独立性，它不能从含等值替换规则 RE 的 **ECK** 系统中被推导出来，故根据 [16] 以及 S 的独立性可知，**ICS** 系统是极小且独立的秘密逻辑系统。

3.3 ICST4 的完全性

将 4 公理 $S\varphi \to SS\varphi$ 加入 **ICST** 系统可得到 **ICST4** 系统（见图4）。[16] **ICST4** 的可靠性可直接从下述命题以及 **ICST** 系统的可靠性中得证。

[13] 易见 **IC** 系统可以从 **K** 系统中推导出来，其中 I 规则可以从单调性规则：从 $\varphi \to \psi$，得 $S\varphi \to S\psi$ 中导出；而 C 公理在 **K** 系统下可导。

[14] 若 $S\top \to S\bot$ 是可推导的，结合 $\neg S\bot$（命题3.3）则有 $\neg S\top$ 是可推导的，与命题3.4相矛盾。

[15] 从 $\vdash \varphi \leftrightarrow \psi$，可得 $\vdash S\varphi \leftrightarrow S\psi$。

[16] 因为秘密信息是“知与不知关系的绑定”，其克里普克模型上的 R_a 与 R_b 关系被当作是主体的“认知不可区分关系”，因而，语义上自然的扩张是向 **S5** 模型逼近，自反传递系统是（已找到的）我们秘密逻辑语言所能刻画的最逼近 **S5**-关系的系统。

命题 3.6 (自反传递性)**.** 4 公理在自反传递的标准框架类（定义如后）上是有效的。(ref)：任给 $w \in W$ 有 $O(w,w,w)$（自反性）；(tran)：任给 $w,u,v \in W$，从 $O(w,u,u)$ 与 $O(u,v,v)$ 可推得 $O(w,v,v)$（传递性）。

证明. 证 $\models S\varphi \to SS\varphi$：反证法。假设有 (M^o,w) 使得 $M^o,w \not\models S\varphi \to SS\varphi$。则有 (1) $M^o,w \models S\varphi$ 但 $M^o,w \not\models SS\varphi$，进一步有 (2) $M^o,w \models \langle S\rangle\langle S\rangle\neg\varphi$。
从 (1)，有对任意的 $u \in W$：
若 $O(w,u,u)$　则 (1.1) $M^o,u \models \varphi$，且　(1.2) 存在 $v \in W$：$O(w,u,v)$ 且 $M,v \models \neg\varphi$。
从 (2)，有 $u \in W$：(*) $O(w,u,u)$ 且
(2.1) $M^o,u \models \langle S\rangle\neg\varphi$，或者　(2.2) 对任意的 $v \in W, O(w,u,v)$ 蕴涵 $M^o,v \models S\varphi$。
再证明上述两种情况中都有矛盾：

- 若 (2.1) 成立。从 $M^o,u \models \langle S\rangle\neg\varphi$ 有存在 $m \in W$, $(^*_*)$ $O(u,m,m)$ 且
  (2.1.1) $M^o,m \models \neg\varphi$，或者　(2.1.2) 对任意的 $n \in W$，$O(u,m,n)$ 蕴涵 $M^o,n \models \varphi$。
  若 (2.1.1) 成立。从 (*) 和 $(^*_*)$，根据 (tran) 则有 $O(w,m,m)$。再根据 (1) 与 (1.1)，有 $M^o,m \models \varphi$，与 (2.1.1) 相矛盾。
  若 (2.1.2) 成立。从 (*) 与 $(^*_*)$，根据 (tran) 有 $O(w,m,m)$。再根据 (1) 与 (1.2)，则存在 $n' \in W$ 使得 $O(w,m,n')$ 与 $M,n' \models \neg\varphi$ 成立。从 $O(u,m,m)$ 以及 $(^*_*)$ 与 $O(w,m,n')$，则根据定义3.3(ii) 有 $O(u,m,n')$。进一步结合 (2.1.2)，则有 $M^o,n' \models \varphi$，与 $M,n' \models \neg\varphi$ 相矛盾。
- 若 (2.2) 成立。即对任意 $v \in W$，$O(w,u,v)$ 蕴涵 $M^o,v \models S\varphi$。从 (*) $O(w,u,u)$，根据 (2.2)（其中 $v=u$）可得 $M^o,u \models S\varphi$。再根据 (ref)，有 $O(u,u,u)$，根据语义定义，有 $M^o,u \models \varphi$ 且 (2.2.1) 存在 $s \in W$ 使得 $O(u,s,s)$ 且 $M^o,s \models \neg\varphi$ 成立。
  从 (*) $O(w,u,u)$ 与 (2.2.1) $O(u,s,s)$，可根据 (tran) 得 $O(w,s,s)$，即有 $M^o,s \models \varphi$（根据 (1) 与 (1.1)），与 (2.2.1) 相矛盾。

故有 $M^o,w \models S\varphi \to SS\varphi$。从 (M^o,w) 的任意性有 $\models S\varphi \to SS\varphi$。　□

ICST4 的完全性与 **ICS** 以及 **ICST** 完全性的证明思路类似，但在构造证明的过程中我们会发现，它不是简单的扩充与推广。首先，我们需要对“带标签的极大一致集”（labelled maximal consistent set）[17]进行筛选，然后对典范关系 O^c 分情况定义，构造一个满足自反性但不保证传递性的标准模型，称为“预模型”（pre-model）；最后在预模型的基础上构造生成真正的典范标准模型（满足自反性与传递性）。

[17]此概念参考了 [16]，目的是通过不同标签的命名，保证每个极大一致集的每个 R_a-后继以及该后继的 R_b-后继都不重叠。比如若 $\Delta[\varphi]$ 的 R_a-后继有 $\Gamma[p]$ 与 $\Gamma[q]$，它们是相同的极大一致集，但由于标签不同，是不同的典范世界且有着不同的 R_b-后继。

令极大一致集为极大 **ICST4**-一致集的简称，$\Gamma[\varphi]$ 是一个带标签的极大一致集，即指 Γ 是极大一致集，且 $\varphi \in \mathcal{L}_S$ 是公式。并有如下定义。

定义 3.8 (预模型)**. ICST4** 上的模型 $M^c = (W^c, O^c, V^c)$ 定义为：

- $W^c = \{\Delta[\varphi] \mid \Delta[\varphi]$ 是带标签的极大一致集，且 $L(\varphi) \in Rab(\Delta)\}$,
- 任给 W^c 中带标签的极大一致集 $\Delta[\chi_1]$、$\Gamma[\chi_2]$ 以及 $\Gamma'[\chi_3]$，有：
  - $O^c(\Delta[\chi_1], \Gamma[\chi_2], \Gamma'[\chi_3])$ 当且仅当 [18]
    - 若 $\Delta = \Gamma$，则 $\Gamma' \in L(\chi_2)$；否则，
    - $\vdash \chi_1 \leftrightarrow \chi_2$，$\Gamma \in Ra(\Delta)$，$L(\chi_2) \in Rab(\Delta)$ 且 $\Gamma' \in L(\chi_2)$。
- 对任意 $p \in$ Prop 有 $V^c(p) = \{\Delta \mid p \in \Delta\}$。

称 $\Gamma[\varphi]$ 是可允许的（admissible），即指 $L(\varphi) \in Rab(\Gamma)$。

由定义 3.8 不难发现，W^c 是所有可允许的带标极大一致集的集合，且对任意的 $\Delta[\chi] \in W^c$，$\varphi \in \Delta[\chi]$ 当且仅当 $\varphi \in \Delta$。故在不影响理解的前提下，将不特别区分 $\varphi \in \Delta$ 与 $\varphi \in \Delta[\chi]$。下面是 **ICST4** 系统中需要反复用到的一些推论。

推论 2 (见 [16])**.** *对任意的基于* **ICST** *系统的极大一致集* Δ *而言,* $S(\Delta)$ *是一致的且* $E(\Delta) \neq \varnothing$*, 此外还有,* $\top \in E(\Delta)$*,* $Ra(\Delta) \neq \varnothing$*, 且* $Rab(\Delta) = \{L(\chi) \mid \chi \in E(\Delta)\}$。

从 [16] 的证明可知，这一推论只依赖于 **ICST** 系统的公理与规则，故在任意由 **ICST** 系统扩张生成的一致系统中，上述推论依旧成立。结合推论 2，定义 3.7 则可有如下简化。

定义 3.9 (定义 3.7 简化)**.** $Ra(\Delta) = \{\Delta' \mid \Delta'$ 是一个极大一致集且 $S(\Delta) \subseteq \Delta'\}$，且 $Rab(\Delta) = \{L(\chi) \mid \chi \in E(\Delta)\}$。

推论 3. *对任意的极大一致集* Γ, Δ*:* $\Gamma \in Ra(\Delta)$ *当且仅当* $S(\Delta) \subseteq S(\Gamma)$*。进一步, 对任意的极大一致集* Δ*, 有* $S(\Delta) \subseteq \Delta$ *且* $\Delta \in Ra(\Delta)$ *。*

证明. ($\Rightarrow$) 假设 $\Gamma \in Ra(\Delta)$，则根据定义 3.9 有 $S(\Delta) \subseteq \Gamma$。再证 $S(\Delta) \subseteq S(\Gamma)$。令 $\varphi \in S(\Delta)$，则有 $S\varphi \in \Delta$（定义 3.6），再根据 4 公理有 $SS\varphi \in \Delta$，故有 $S\varphi \in S(\Delta)$，从 $S(\Delta) \subseteq \Gamma$ 有 $S\varphi \in \Gamma$，据定义 3.6 有 $\varphi \in S(\Gamma)$。

($\Leftarrow$) 假设 $S(\Delta) \subseteq S(\Gamma)$。若有 (*) $S(\Delta) \subseteq \Gamma$，则有 $\Gamma \in Ra(\Delta)$（定义 3.9）。再证明 (*) $S(\Delta) \subseteq \Gamma$：令 $\varphi \in S(\Delta)$，则从假设 $S(\Delta) \subseteq S(\Gamma)$ 中有 $\varphi \in S(\Gamma)$，故有 $S\varphi \in \Gamma$，根据 T 公理有 $\varphi \in \Gamma$，(*) 得证。故第一个命题得证。

[18] 与 **ICST** 的典范标准模型定义不同，我们分情况考虑了 Γ 与 Δ 是否等同的情况。当 $\Gamma = \Delta$ 时对典范关系要求弱化了，只要求 $\Gamma' \in L(\chi_2)$；而当 $\Gamma \neq \Delta$ 时，则额外要求了 $\vdash \chi_1 \leftrightarrow \chi_2$。这样的设置是为了技术上构造条件保证传递性：具体而言，是为了将预模型扩展为典范标准模型时，有条件确保标准模型的传递性。

结合 $S(\Delta) \subseteq S(\Delta)$，根据已证命题可知，$\Delta \in Ra(\Delta)$，故有 $S(\Delta) \subseteq \Delta$（定义 3.9）。 □

从定义 3.9、推论 3 以及推论 2，可有如下推论。

推论 4. 若 $\Delta[\chi]$ 是可允许的（即 $L(\chi) \in Rab(\Delta)$），则 $\Delta \in L(\chi)$。特别而言，对任意极大一致集 Δ，有 $\Delta[\top]$ 是可允许的。

证明. 若 $\Delta[\chi]$ 是可允许的，即 $L(\chi) \in Rab(\Delta)$，根据定义 3.9，$\chi \in E(\Delta)$，根据定义3.6，有 $S(\Delta) \vdash \chi$。从 $S(\Delta) \subseteq \Delta$（推论 3），有 $\Delta \vdash \chi$，从 Δ 是极大一致集有 $\chi \in \Delta$，故有 $\Delta \in L(\chi)$（定义 3.6）。

从推论 2，可知 $\top \in E(\Delta)$ 且对任意的极大一致集 Δ 有 $Ra(\Delta) \neq \varnothing$。根据定义 3.9有 $L(\top) \in Rab(\Delta)$，即 $\Delta[\top]$ 是可允许的。 □

推论 5. 对任意的 $\chi_1, \chi_2, \chi_3 \in \mathcal{L}_S$，若 $O^c(\Delta[\chi_1], \Gamma[\chi_2], \Gamma'[\chi_3])$ 则 $\Gamma \in Ra(\Delta)$，$L(\chi_2) \in Rab(\Delta)$ 且 $\Gamma' \in L(\chi_2)$。

证明. 令 $O^c(\Delta[\chi_1], \Gamma[\chi_2], \Gamma'[\chi_3])$。若 $\Delta \neq \Gamma$，根据定义 3.8，推论显然成立。若 $\Delta = \Gamma$，则有 $O^c(\Delta[\chi_1], \Delta[\chi_2], \Gamma'[\chi_3])$，根据定义 3.8 可得 $\Gamma' \in L(\chi_2)$。只需再证 $\Delta \in Ra(\Delta)$ 且 $L(\chi_2) \in Rab(\Delta)$。再从 $\Delta[\chi_2]$ 是可允许的（定义 3.8），故有 $L(\chi_2) \in Rab(\Delta)$（推论 4），且有 $\Delta \in Ra(\Delta)$（推论 3）。 □

至此，可证明定义 3.8 给出的典范标准模型是满足自反性的标准模型。

命题 3.7 (预典范性). 定义 3.8 给出的 $M^c = (W^c, O^c, V^c)$ 满足如下性质：

(1) 存在 $\Gamma'[\chi_3] \in W^c$ 使得 $O^c(\Delta[\chi_1], \Gamma[\chi_2], \Gamma'[\chi_3])$ 当且仅当 $O^c(\Delta[\chi_1], \Gamma[\chi_2], \Gamma[\chi_2])$。
(2) 对任意 $\chi, \chi_1, \chi_2, \delta, \delta' \in \mathcal{L}_S$：
若 $O^c(\Delta[\chi_1], \Gamma[\chi], \Omega[\delta])$ 且 $O^c(\Delta'[\chi_2], \Gamma[\chi], \Omega'[\delta'])$，则 $O^c(\Delta[\chi_1], \Gamma[\chi], \Omega'[\delta'])$。
(3) 对任意 $\Delta[\chi] \in W^c$：$O^c(\Delta[\chi], \Delta[\chi], \Delta[\chi])$。

证明. (1) ($\Rightarrow$) 不论 $\Gamma = \Delta$ 是否成立，只需证明 $\Gamma \in L(\chi_2)$。它可直接从推论 4 与 $\Gamma[\chi_2]$ 的可允许性中得出。($\Leftarrow$) 显然。

(2) 假设 (a) $O^c(\Delta[\chi_1], \Gamma[\chi], \Omega[\delta])$ 且 (b) $O^c(\Delta'[\chi_2], \Gamma[\chi], \Omega'[\delta'])$ 成立，需证明 $O^c(\Delta[\chi_1], \Gamma[\chi], \Omega'[\delta'])$ 成立。考虑如下两种情况：

- 若 $\Delta = \Gamma$：从 (b) 可得 $\Omega' \in L(\chi)$，故有 $O^c(\Delta[\chi_1], \Gamma[\chi], \Omega'[\delta'])$。
- 若 $\Delta \neq \Gamma$：我们证明 (1) $\vdash \chi_1 \leftrightarrow \chi$，(2) $\Gamma \in Ra(\Delta)$，(3) $L(\chi) \in Rab(\Delta)$ 以及 (4) $\Omega' \in L(\chi)$。通过观察定义 3.8，(1)，(2)，(3) 可直接从 (a) 中推出。而 (4) 则可从 (b) 中推出，故有 $O^c(\Delta[\chi_1], \Gamma[\chi], \Omega'[\delta'])$ 成立。

(3) 任给 $\Delta[\chi] \in W^c$，即有 $L(\chi) \in Rab(\Delta)$，故 $\Delta \in L(\chi)$（推论 4）。 □

命题 3.7 只证明了定义 3.8 中给出的 M^c 是自反的标准模型，其并不保证一定具有传递性。令 $O^c(\Delta[\chi_1],\Gamma[\chi'],\Gamma[\chi'])$ 且 $O^c(\Gamma[\chi'],\Gamma[\chi_2],\Gamma[\chi_2])$，不能保证有 $O^c(\Delta[\chi_1],\Gamma[\chi_2],\Gamma[\chi_2])$。因为从 $L(\chi_2)\in Rab(\Gamma)$ 并不必然有 $L(\chi_2)\in Rab(\Delta)$。这是因为，从 $S(\Delta)\subseteq S(\Gamma)$ 不能保证有：$S(\Gamma)\vdash\chi_2$ 蕴涵 $S(\Delta)\vdash\chi_2$。所以，M^c 不是 **ICST4** 系统的模型，它只是一个 预模型。为了保证传递性，我们需要对预模型 M^c 进行扩张。

定义 3.10 (典范标准模型)**.** 在预模型 M^c 上定义（**ICST4** 上）典范标准模型 $M^e=(W^e,O^e,V^e)$ 如下：

- $W^e=W^c$，且对任意 $p\in$ Prop，$V^e(p)=V^c(p)$。
  对任意 W^e 中的元素而言：
- $O^e(\Delta[\chi_1],\Gamma[\chi_2],\Gamma'[\chi_3])$ 当且仅当存在 $\chi'\in\mathcal{L}_S$ 使得
  $O^c(\Delta[\chi_1],\Delta[\chi'],\Delta[\chi'])$，$O^c(\Delta[\chi'],\Gamma[\chi'],\Gamma[\chi'])$ 且 $O^c(\Gamma[\chi'],\Gamma[\chi_2],\Gamma'[\chi_3])$。

下面，我们证明 M^e 模型只是 M^c 模型在 O^c 关系上的保守扩展。

命题 3.8 (保守扩展性)**.** 对任意的 W^e 中的元素，有如下性质：
(1) 若 $O^c(\Delta[\chi_1],\Gamma[\chi_2],\Gamma'[\chi_3])$，则 $O^e(\Delta[\chi_1],\Gamma[\chi_2],\Gamma'[\chi_3])$。
(2) $O^c(\Delta[\chi_1],\Delta[\chi_2],\Delta[\chi_2])$ 当且仅当 $O^e(\Delta[\chi_1],\Delta[\chi_2],\Delta[\chi_2])$。

证明. (1) 令 $O^c(\Delta[\chi_1],\Gamma[\chi_2],\Gamma'[\chi_3])$。我们先证：
(a) $O^c(\Delta[\chi_1],\Delta[\chi_2],\Delta[\chi_2])$, (b) $O^c(\Delta[\chi_2],\Gamma[\chi_2],\Gamma[\chi_2])$ 且 (c) $O^c(\Gamma[\chi_2],\Gamma[\chi_2],\Gamma'[\chi_3])$。

(a) 根据 $O^c(\Delta[\chi_1],\Gamma[\chi_2],\Gamma'[\chi_3])$ 有 $L(\chi_2)\in Rab(\Delta)$（推论 5），即知 $\Delta[\chi_2]\in W^e$。从 $O^c(\Delta[\chi_1],\Gamma[\chi_2],\Gamma'[\chi_3])$ 亦可知 $\Delta[\chi_1]\in W^e$，由 $L(\chi_2)\in Rab(\Delta)$ 与推论 4 又有 $\Delta\in L(\chi_2)$。据定义 3.8 有 $O^c(\Delta[\chi_1],\Delta[\chi_2],\Delta[\chi_2])$ 成立。

(b) 根据 $O^c(\Delta[\chi_1],\Gamma[\chi_2],\Gamma'[\chi_3])$ 有 $\Gamma[\chi_2]$ 是可允许的，即 $\Gamma\in L(\chi_2)$。根据定义 3.8，若 $\Delta=\Gamma$，则 (b) 成立；若 $\Delta\neq\Gamma$，则从 $O^c(\Delta[\chi_1],\Gamma[\chi_2],\Gamma'[\chi_3])$ 中可知 $\Gamma\in Ra(\Delta)$ 与 $L(\chi_2)\in Rab(\Delta)$ 成立（推论 5）。又有 $\vdash\chi_2\leftrightarrow\chi_2$ 且 $\Gamma\in L(\chi_2)$，所以 (b) 成立（定义 3.8）。

(c) 从 $O^c(\Delta[\chi_1],\Gamma[\chi_2],\Gamma'[\chi_3])$ 中可知 $\Gamma[\chi_2]$ 是可允许的且 $\Gamma'\in L(\chi_2)$（定义 3.8），故 (c) $O^c(\Gamma[\chi_2],\Gamma[\chi_2],\Gamma'[\chi_3])$ 成立。

由 (a)、(b) 以及 (c) 可知，根据定义 3.10，令 $\chi'=\chi_2$ 时，有 $O^e(\Delta[\chi_1],\Gamma[\chi_2],\Gamma'[\chi_3])$。

(2) ($\Rightarrow$) 由命题 3.8(1) 所保证。($\Leftarrow$) 若 $O^e(\Delta[\chi_1],\Delta[\chi_2],\Delta[\chi_2])$，则有 $O^c(\Delta[\chi'],\Delta[\chi'],\Delta[\chi'])$ 且 $O^c(\Delta[\chi'],\Delta[\chi_2],\Delta[\chi_2])$。从 $\Delta\in L(\chi_2)$、$\Delta[\chi_1]\in W^e$、$\Delta[\chi_2]\in W^e$ 与定义 3.8 中可推出 $O^c(\Delta[\chi_1],\Delta[\chi_2],\Delta[\chi_2])$。 □

命题 3.8 证明了 M^e 是 M^c 的保守扩展。现在，证明 M^e 的确是满足自反性与传递性的标准模型。

命题 3.9 (典范性). **ICST4** 的典范标准模型 $M^e = (W^e, O^e, V^e)$ 满足如下四条性质：

(1) 存在 $\Gamma'[\chi_3] \in W^e$ 使得 $O^e(\Delta[\chi_1], \Gamma[\chi_2], \Gamma'[\chi_3])$ 当且仅当 $O^e(\Delta[\chi_1], \Gamma[\chi_2], \Gamma[\chi_2])$。

(2) 对任意 $\chi, \chi_1, \chi_2, \delta, \delta', \in \mathcal{L}_S$：

若 $O^e(\Delta[\chi_1], \Gamma[\chi], \Omega[\delta])$ 且 $O^e(\Delta'[\chi_2], \Gamma[\chi], \Omega'[\delta'])$，则 $O^e(\Delta[\chi_1], \Gamma[\chi], \Omega'[\delta'])$。

(3) 对任意 $\Delta[\chi] \in W^e$：$O^e(\Delta[\chi], \Delta[\chi], \Delta[\chi])$。

(4) 对任意 $\Delta[\chi_1], \Gamma[\chi_2], \Omega[\chi_3] \in W^e$：

若 $O^e(\Delta[\chi_1], \Gamma[\chi_2], \Gamma[\chi_2])$ 且 $O^e(\Gamma[\chi_2], \Omega[\chi_3], \Omega[\chi_3])$，则 $O^e(\Delta[\chi_1], \Omega[\chi_3], \Omega[\chi_3])$。

证明. 这里 (1) 和 (2) 对应了标准模型的基本属性，(3) 和 (4) 则分别对应了标准模型的自反性与传递性。

(1) (⇒)

$O^e(\Delta[\chi_1], \Gamma[\chi_2], \Gamma'[\chi_3])$

⇒ 存在 χ' 使得 $O^c(\Delta[\chi_1], \Delta[\chi'], \Delta[\chi'])$，

$O^c(\Delta[\chi'], \Gamma[\chi'], \Gamma[\chi'])$ 且 $O^c(\Gamma[\chi'], \Gamma[\chi_2], \Gamma'[\chi_3])$。　定义 3.10

⇒ 存在 χ' 使得 $O^c(\Delta[\chi_1], \Delta[\chi'], \Delta[\chi'])$，

$O^c(\Delta[\chi'], \Gamma[\chi'], \Gamma[\chi'])$ 且 $O^c(\Gamma[\chi'], \Gamma[\chi_2], \Gamma[\chi_2])$。　命题 3.7(1)

⇒ $O^e(\Delta[\chi_1], \Gamma[\chi_2], \Gamma[\chi_2])$。　定义 3.10

(⇐) 显然。

(2) 假设 1) $O^e(\Delta[\chi_1], \Gamma[\chi], \Omega[\delta])$ 且 2) $O^e(\Delta'[\chi_2], \Gamma[\chi], \Omega'[\delta'])$ 成立，

需证 $O^e(\Delta[\chi_1], \Gamma[\chi], \Omega'[\delta'])$。根据定义3.10有：

从 1) 有　(a) 存在 χ' 使得 $O^c(\Delta[\chi_1], \Delta[\chi'], \Delta[\chi'])$，$O^c(\Delta[\chi'], \Gamma[\chi'], \Gamma[\chi'])$ 且 $O^c(\Gamma[\chi'], \Gamma[\chi], \Omega[\delta])$。

从 2) 有　(b) 存在 χ'' 使得 $O^c(\Delta'[\chi_2], \Delta'[\chi''], \Delta'[\chi''])$，$O^c(\Delta'[\chi''], \Gamma[\chi''], \Gamma[\chi''])$ 且 $O^c(\Gamma[\chi''], \Gamma[\chi], \Omega'[\delta'])$。

要证 $O^e(\Delta[\chi_1], \Gamma[\chi], \Omega'[\delta'])$，我们证明存在 χ''' 使得：

$O^c(\Delta[\chi_1], \Delta[\chi'''], \Delta[\chi'''])$, $O^c(\Delta[\chi'''], \Gamma[\chi'''], \Gamma[\chi'''])$ 且 $O^c(\Gamma[\chi'''], \Gamma[\chi], \Omega'[\delta'])$。

只需证明当 $\chi''' = \top$ 时，如下成立：

(2.1) $O^c(\Delta[\chi_1], \Delta[\top], \Delta[\top])$，(2.2) $O^c(\Delta[\top], \Gamma[\top], \Gamma[\top])$ 且 (2.3) $O^c(\Gamma[\top], \Gamma[\chi], \Omega'[\delta'])$。

因为 $\Delta[\chi_1]$ 与 $\Gamma[\chi]$ 从 (a) 可知是可允许的，故从 $\Delta \in L(\top)$ 根据定义 3.8 有 (2.1) 成立。当 $\Delta \neq \Gamma$，从 (a) 亦可知 $\Gamma \in Ra(\Delta)$（推论 5），且 $L(\top) \in Rab(\Delta)$（推论 2）以及 $\Gamma \in L(\top)$（定义 3.6），故据定义 3.8 有 (2.2) 成立（当 $\Delta = \Gamma$ 时，可由命题 3.7(3) 与 $\Delta[\top]$ 是可允许的保证）。从 (b) 有 $\Omega' \in L(\chi)$（推论 5），且 $\Gamma[\chi]$ 与 $\Omega'[\delta']$ 是可允许的，故据定义 3.8有 (2.3) 成立。

(3) 根据命题 3.8(2)，只需证 $O^c(\Delta[\chi], \Delta[\chi], \Delta[\chi])$，其由命题 3.7(3) 所保证。

(4) 令 1) $O^e(\Delta[\chi_1], \Gamma[\chi_2], \Gamma[\chi_2])$ 与 2) $O^e(\Gamma[\chi_2], \Omega[\chi_3], \Omega[\chi_3])$ 成立，

我们证明 $O^e(\Delta[\chi_1], \Omega[\chi_3], \Omega[\chi_3])$ 成立。首先，根据定义 3.10，

从 1) 有 (a) 存在 χ' 使得 $O^c(\Delta[\chi_1], \Delta[\chi'], \Delta[\chi'])$，$O^c(\Delta[\chi'], \Gamma[\chi'], \Gamma[\chi'])$ 且 $O^c(\Gamma[\chi'], \Gamma[\chi_2], \Gamma[\chi_2])$。

从 2) 有 (b) 存在 χ'' 使得 $O^c(\Gamma[\chi_2], \Gamma[\chi''], \Gamma[\chi''])$，$O^c(\Gamma[\chi''], \Omega[\chi''], \Omega[\chi''])$ 且 $O^c(\Omega[\chi''], \Omega[\chi_3], \Omega[\chi_3])$。

对于 $O^e(\Delta[\chi_1], \Omega[\chi_3], \Omega[\chi_3])$，则证明存在 χ''' 使得 $O^c(\Delta[\chi_1], \Delta[\chi'''], \Delta[\chi'''])$，$O^c(\Delta[\chi'''], \Omega[\chi'''], \Omega[\chi'''])$ 且 $O^c(\Omega[\chi'''], \Omega[\chi_3], \Omega[\chi_3])$。

令 $\chi''' = \top$，则只需证：

(4.1) $O^c(\Delta[\chi_1], \Delta[\top], \Delta[\top])$，(4.2) $O^c(\Delta[\top], \Omega[\top], \Omega[\top])$ 且 (4.3) $O^c(\Omega[\top], \Omega[\chi_3], \Omega[\chi_3])$。

(4.1) 根据 (a) 有 $\Delta[\chi_1]$ 是可允许的。$\Delta[\top]$ 是可允许的（推论 4）且 $\Delta \in L(\top)$（定义 3.6），据定义 3.8，有 $O^c(\Delta[\chi_1], \Delta[\top], \Delta[\top])$ 成立。

(4.2) 易知 $\Delta[\top]$ 与 $\Omega[\top]$ 是可允许的（推论 4）。$L(\top) \in Rab(\Delta)$（推论 2）与 $\Omega \in L(\top)$（定义 3.6）成立。若有 $\Omega \in Ra(\Delta)$，则根据定义 3.8 有 (4.2) 恒成立。现证 $\Omega \in Ra(\Delta)$：根据推论 5，从 (a) 可知 $\Gamma \in Ra(\Delta)$；从 (b) 可知 $\Omega \in Ra(\Gamma)$。再根据推论 3 有 $S(\Delta) \subseteq S(\Gamma)$ 且 $S(\Gamma) \subseteq S(\Omega)$。从而有 $S(\Delta) \subseteq S(\Omega)$，即有 $\Omega \in Ra(\Delta)$ 成立（推论 3）。

(4.3) 根据推论 4 有 $\Omega[\top]$ 是可允许的，同样，由 (b) 可知 $\Omega[\chi_3]$ 也是可允许的。$\Omega \in L(\chi_3)$ 与 $L(\chi_3) \in Rab(\Omega)$ 则可从 (b) 与推论 5 中得出。所以，根据定义 3.8，(4.3) 成立。

故，从 (4.1)，(4.2)，(4.3) 有 $O^e(\Delta[\chi_1], \Omega[\chi_3], \Omega[\chi_3])$ 成立（定义 3.10）。 □

为了便于存在引理的证明，我们先证如下命题。

命题 3.10. *若 $O^e(\Delta[\chi_1], \Gamma[\chi_2], \Gamma'[\chi])$ 则 $\Gamma \in Ra(\Delta)$ 且 $\Gamma' \in L(\chi_2)$。*

证明. 给定 $O^e(\Delta[\chi_1], \Gamma[\chi_2], \Gamma'[\chi])$，则有 $\chi' \in \mathcal{L}_S$ 使得 $O^c(\Delta[\chi_1], \Delta[\chi'], \Delta[\chi'])$，(1) $O^c(\Delta[\chi'], \Gamma[\chi'], \Gamma[\chi'])$ 且 (2) $O^c(\Gamma[\chi'], \Gamma[\chi_2], \Gamma'[\chi])$（定义 3.10）；根据推论 5，从 (1) 有 $\Gamma \in Ra(\Delta)$，从 (2) 有 $\Gamma' \in L(\chi_2)$。 □

下面我们可证明扩张的典范标准模型 M^e 对模态算子封闭。

引理 3.4 (存在引理)**.** *对任意 $\Delta[\chi_1] \in W^e$，如果 $\langle S\rangle\varphi \in \Delta[\chi_1]$，那么存在 $\Gamma[\chi]$ 使得 $O^e(\Delta[\chi_1], \Gamma[\chi], \Gamma[\chi])$ 且 [$\varphi \in \Gamma[\chi]$，或者对任意 $\Gamma'[\chi_3]$ 有，如果 $O^e(\Delta[\chi_1], \Gamma[\chi], \Gamma'[\chi_3])$，那么 $\neg\varphi \in \Gamma'[\chi_3]$]。*

证明. 令 $\Delta[\chi_1] \in W^e$ 且 $\langle S\rangle\varphi \in \Delta[\chi_1]$。据定义 3.9 可知，$Rab(\Delta) = \{L(\chi) \mid \chi \in E(\Delta)\}$。根据 $\varphi \in N(\Delta)$，讨论以下两种情况：

- 若 $\neg\varphi \in E(\Delta)$，则 $L(\neg\varphi) \in Rab(\Delta)$。从定义 3.8 有 $O^c(\Delta[\chi_1], \Delta[\neg\varphi], \Delta[\neg\varphi])$，再根据命题 3.8(2)，有 $O^e(\Delta[\chi_1], \Delta[\neg\varphi], \Delta[\neg\varphi])$。对任意 $\Gamma'[\chi_3] \in W^e$ 而

言，根据命题 3.10，从 $O^e(\Delta[\chi_1],\Delta[\neg\varphi],\Gamma'[\chi_3])$ 可得 $\Gamma' \in L(\neg\varphi)$。故有 $O^e(\Delta[\chi_1],\Delta[\neg\varphi],\Gamma'[\chi_3])$ 蕴涵 $\neg\varphi \in \Gamma'$（定义 3.6）。

- 若 $\neg\varphi \notin E(\Delta)$，则从 $\varphi \in N(\Delta)$，有 $S(\Delta) \nvdash \neg\varphi$（定义 3.6），所以 $S(\Delta)\cup\{\varphi\}$ 是一致的。从 $S(\Delta)\cup\{\varphi\}$ 中生成一个极大一致集 Γ，则有 $S(\Delta)\subseteq\Gamma$，据定义 3.9，有 $\Gamma \in Ra(\Delta)$。从推论 2 有 $L(\top) \in Rab(\Delta)$，且 $\varphi \in \Gamma[\top]$（根据构造）。现证明 (*) $O^e(\Delta[\chi_1],\Gamma[\top],\Gamma[\top])$ 成立。若有 $O^c(\Delta[\chi_1],\Gamma[\top],\Gamma[\top])$ 成立，则根据命题 3.8(1) 则有 (*) 成立。已知 $\Delta[\chi_1]$（前提）与 $\Gamma[\top]$（推论 4）都是可允许的。从 $\Gamma \in Ra(\Delta)$，$L(\top) \in Rab(\Delta)$ 以及 $\Gamma \in L(\top)$ 可根据定义 3.8 推得 $O^c(\Delta[\chi_1],\Gamma[\top],\Gamma[\top])$ 成立。所以，有 $O^e(\Delta[\chi_1],\Gamma[\top],\Gamma[\top])$ 且 $\varphi \in \Gamma[\top]$。

故该引理得证。 □

为了证明真值引理，需先证明如下前置命题。

命题 3.11. *若 $O^e(\Delta[\chi_1],\Gamma[\chi],\Gamma[\chi])$ 且 [$\psi \in \Gamma[\chi]$,或者对任意 $\Gamma'[\chi_3] \in W^e$:$O^e(\Delta[\chi_1],\Gamma[\chi],\Gamma'[\chi_3])$ 蕴涵 $\psi \in \Gamma'[\chi_3]$]，则 $\langle S\rangle\psi \in \Delta[\chi_1]$。*

证明.（证其逆否命题）令 $\langle S\rangle\psi \notin \Delta[\chi_1]$,则根据极大一致集属性与对偶性有 $S\neg\psi \in \Delta[\chi_1]$。再证明：

对任意 $\Gamma[\chi] \in W^e$，若 $O^e(\Delta[\chi_1],\Gamma[\chi],\Gamma[\chi])$ 则 $\neg\psi \in \Gamma[\chi]$ 且存在 $\Gamma'[\chi_3] \in W^e$: $O^e(\Delta[\chi_1],\Gamma[\chi],\Gamma'[\chi_3])$ *且 $\psi \in \Gamma'[\chi_3]$。*

假设 $O^e(\Delta[\chi_1],\Gamma[\chi],\Gamma[\chi])$，则根据命题 3.10 有 $\Gamma \in Ra(\Delta)$，且 $\Gamma \in L(\chi)$，故有 $\Gamma[\chi]$ 是可允许的。从 $\Gamma \in Ra(\Delta)$ 可得 $S(\Delta)\subseteq S(\Gamma)$（推论 3），再从 $S\neg\psi \in \Delta[\chi_1]$ 中可得 $\neg\psi \in S(\Delta)$，故有 $\neg\psi \in S(\Gamma)$，则 $S\neg\psi \in \Gamma[\chi]$，根据 T 公理，有 $\neg\psi \in \Gamma[\chi]$。

从 $O^e(\Delta[\chi_1],\Gamma[\chi],\Gamma[\chi])$ 根据定义 3.10 可知存在 $\chi' \in \mathcal{L}_S$，

(1) $O^c(\Delta[\chi_1],\Delta[\chi'],\Delta[\chi'])$，(2) $O^c(\Delta[\chi'],\Gamma[\chi'],\Gamma[\chi'])$ 且 (3) $O^c(\Gamma[\chi'],\Gamma[\chi],\Gamma[\chi])$。

从推论2可知 $S(\Gamma)$ 是一致集，且又根据定义3.9有 $Rab(\Gamma) = \{L(\chi) \mid \chi \in E(\Gamma)\}$。故从命题 3.2 可知，$\{\neg\neg\psi,\chi\}$ 是一致的（其中 $\neg\psi \in S(\Gamma)$，χ 为 $E(\Gamma)$ 中任意元素，由推论 2 知 $E(\Gamma)\neq\varnothing$）。故，对由 $\{\neg\neg\psi,\chi\}$ 生成的任意极大一致集 Γ'，有 $\Gamma' \in L(\chi)$ 且 $\psi \in \Gamma'$。故从 (3) 可得 $\Gamma[\chi']$、$\Gamma[\chi]$ 是可允许的，故据定义 3.8 有 (4) $O^c(\Gamma[\chi'],\Gamma[\chi],\Gamma'[\chi])$。结合 (1)、(2) 以及 (4) 有 $O^e(\Delta[\chi_1],\Gamma[\chi],\Gamma'[\chi])$ 且 $\psi \in \Gamma'[\chi]$（定义 3.10，其中 $\chi_3 = \chi$）。

故我们证明了对任意 $\Gamma[\chi] \in W^e$，若 $O^e(\Delta[\chi_1],\Gamma[\chi],\Gamma[\chi])$ 则 $\neg\psi \in \Gamma[\chi]$ 且存在 $\Gamma'[\chi_3] \in W^e$：$O^e(\Delta[\chi_1],\Gamma[\chi],\Gamma'[\chi_3])$ 且 $\psi \in \Gamma'[\chi_3]$。 □

引理 3.5 (真值引理)**.** *令 $M^e = (W^e, O^e, V^e)$ 为典范标准模型。则有：对任意的 $\varphi \in \mathcal{L}_S$ 以及 $\Delta[\chi_1] \in W^e$，$M^e,\Delta[\chi_1] \models \varphi$ 当且仅当 $\varphi \in \Delta[\chi_1]$。*

证明. 只考虑模态公式 $\varphi = \langle S\rangle\psi$ 的情形，其他情形略。

(⇒) 若 $M^e, \Delta[\chi_1] \models \langle S\rangle\psi$，则存在 $\Gamma[\chi] \in W^e$ 使得 $O^e(\Delta[\chi_1], \Gamma[\chi], \Gamma[\chi])$ 且 [$M^e, \Gamma[\chi] \models \psi$，或者对任意 $\Gamma'[\chi_2] \in W^e$，$O^e(\Delta[\chi_1], \Gamma[\chi], \Gamma'[\chi_2])$ 蕴涵 $M^e, \Gamma'[\chi_2] \models \neg\psi$]。据归纳假设，存在 $\Gamma[\chi] \in W^e$ 使得 $O^e(\Delta[\chi_1], \Gamma[\chi], \Gamma[\chi])$ 且 [$\psi \in \Gamma[\chi]$，或者对任意 $\Gamma'[\chi_2] \in W$，$O^e(\Delta[\chi_1], \Gamma[\chi], \Gamma'[\chi_2])$ 蕴涵 $\neg\psi \in \Gamma'[\chi_2]$]。从命题 3.11 可得 $\langle S\rangle\psi \in \Delta[\chi_1]$。

(⇐) 若 $\langle S\rangle\psi \in \Delta[\chi_1]$，根据引理 3.4，存在 $\Gamma[\chi]$ 使得 $O^e(\Delta[\chi_1], \Gamma[\chi], \Gamma[\chi])$ 且 [$\psi \in \Gamma[\chi]$，或者对任意 $\Gamma'[\chi_2]$，$O^e(\Delta[\chi_1], \Gamma[\chi], \Gamma'[\chi_2])$ 蕴涵 $\neg\psi \in \Gamma'[\chi_2]$]。即有存在 $\Gamma[\chi]$，$O^e(\Delta[\chi_1], \Gamma[\chi], \Gamma[\chi])$ 且 [$M^e, \Gamma[\chi] \models \psi$（归纳假设），或者对任意 $\Gamma'[\chi_2]$，$O^e(\Delta[\chi_1], \Gamma[\chi], \Gamma'[\chi_2])$ 蕴涵 $M^e, \Gamma'[\chi_2] \models \neg\psi$（归纳假设）]。根据语义定义，$M^e, \Delta[\chi_1] \models \langle S\rangle\psi$。 □

从真值引理易得如下推论。

推论 6. *对任意 $\Delta[\chi_1], \Delta[\chi_2] \in W^e$ 以及任意 $\varphi \in \mathcal{L}_S$, $M^e, \Delta[\chi_1] \models \varphi$ 当且仅当 $M^e, \Delta[\chi_2] \models \varphi$。*

证明. 假设 $\Delta[\chi_1], \Delta[\chi_2] \in W^e$ 且 $\varphi \in \mathcal{L}_S$ 都是任意的。$M^e, \Delta[\chi_1] \models \varphi$，当且仅当 $\varphi \in \Delta[\chi_1]$（引理3.5），当且仅当 $\varphi \in \Delta[\chi_2]$（带标签的极大一致集的定义），当且仅当 $M^e, \Delta[\chi_2] \models \varphi$（引理 3.5）。 □

定理 3.6 (标准框架完全性)**. ICST4** *对于满足自反与传递关系的标准框架类*[19]*是强完全的。*

证明.（证其逆否命题）令 $\Omega \nvdash_{\mathbf{ICST4}} \varphi$，则 $\Omega \cup \{\neg\varphi\}$ 是 **ICST4**-一致的。将其生成为一个极大且 **ICST4**-一致的集合 Ω'，再据引理 3.5，$M^e, \Omega'[\top] \models \neg\varphi$（据推论 4，$\Omega'[\top]$ 是可允许的），故有 $\Omega \not\models \neg\varphi$。同时，我们也在命题 3.9 中证明了 M^e 是满足自反性与传递性的标准模型，故该定理得证。 □

根据定理 3.1，可进一步证明基于秘密框架类（二元关系的克里普克框架）上的完全性结果。

定理 3.7 (完全性)**. ICST4** *是对任意满足 R_a-自反性（$\forall x R_a(x, x)$）以及 R_a-传递性（$\forall x\forall y\forall z((R_a(x, y) \wedge R_a(y, z)) \to R_a(x, z))$）秘密框架而言是强完全的。*

证明. 根据对定理 3.6 的证明，有 $M^e, \Omega'[\top] \models \neg\varphi$。进一步，$Tr(M^e), \Omega'[\top] \models \neg\varphi$（定理 3.1）。再证 $Tr(M^e)$ 是一个满足 R_a-自反性与 R_a-传递性的秘密模型。

（**R_a-自反性**）根据命题3.9(3) 可知，对任意 $\Delta[\chi] \in W^e$：$O^e(\Delta[\chi], \Delta[\chi], \Delta[\chi])$。故据定义3.5，有 $\Delta[\chi] R_a \Delta[\chi]$。

（**R_a-传递性**）令有 $\Delta[\chi_1], \Gamma[\chi_2], \Omega[\chi_3] \in W^e$，$\Delta[\chi_1] R_a \Gamma[\chi_2]$ 以及 $\Gamma[\chi_2] R_a \Omega[\chi_3]$。据定义 3.5，则有 $\Gamma'[\delta'], \Gamma''[\delta''] \in W^e$ 使得 $O^e(\Delta[\chi_1], \Gamma[\chi_2], \Gamma'[\delta'])$ 且 $O^e(\Gamma[\chi_2], \Omega[\chi_3],$

[19] 分别为 $\forall x O(x, x, x)$ 与 $\forall x\forall y\forall z((O(x, y, y) \wedge O(y, z, z)) \to O(x, z, z))$。

$\Gamma''[\delta'']$)。从而有 $O^e(\Delta[\chi_1],\Gamma[\chi_2],\Gamma[\chi_2])$ 且 $O^e(\Gamma[\chi_2],\Omega[\chi_3],\Omega[\chi_3])$（命题 3.9(1)），据 O^e-传递性，有 $O^e(\Delta[\chi_1],\Omega[\chi_3],\Omega[\chi_3])$，再据定义 3.5 有 $\Delta[\chi_1]R_a\Omega[\chi_3]$。 □

3.4 ICST4 的讨论

根据命题 3.5 可知，5 公理在 **ST** 系统下不一致，故有：**ICST5** 以及 **ICST45** 系统都是不可靠的系统。即 **ICST4** 系统是（R_a 与 R_b）自反的秘密逻辑系统 **ICST** 在知识公理下极大一致的扩展，秘密模态对负自省公理不保持有效性。本文证明了秘密逻辑系统 **ICST4** 在 R_a-自反且 R_a-传递的框架类（**S4**）上是有效的，但基于等价框架（**S5**）上的秘密逻辑系统（不含 5 公理）还有待进一步研究，其主要难点在于秘密模态的 5 公理（$\neg S_a\varphi \to S_a\neg S_a\varphi$）在 **S5** 模型上不是有效式，在纯秘密逻辑 $\mathcal{L}_S$ 上，欧性或对称性是否可以被刻画还有待进一步分析，需要考察纯秘密逻辑的表达力问题等。[12] 给出了 **ECK** 与 **EK** 系统邻域语义上的完全性证明，但没有给出 **ECK4** 系统的完全性证明。**ICST4** 系统可以看成是对 **ECKT4** 系统的简单扩展（将其等值替换规则 RE 替换成了插值规则 I，再额外引入了 S 公理）。[20]（带标签的）典范模型方法或许也可以用于对 **ECKT4** 系统完全性的构造与证明。

本节参照知识逻辑公理系统 **S5**，对（单主体系统）纯秘密逻辑扩张进行了讨论。**ICST4** 在 **S4** 系统下是可靠完全的。文中涉及的“主体 b”可以看成任意不同于 a 的主体，且 **ICST** 系统在 R_a-自反与 R_b-自反的克里普克框架类下是可靠且强完全的（R_b-自反的框架与非 R_b-自反的框架逻辑等价，见 [16]）；但我们不能断定 **ICST4** 系统在 R_a 与 R_b 都自反且传递的框架系统下是完全的（可能不是完全的，因为 R_b-传递框架与非 R_b-传递框架在语言 $\mathcal{L}_S$ 下并不逻辑等价），我们猜测 $\mathcal{L}_S$ 语言是无法刻画 R_b-关系的（因为没有直接反映 R_b 关系的模态公式，如 $S_b\varphi$），讨论所有主体认知关系都是自反且传递的逻辑系统，需要放开对确定单主体的限制，允许有形如 $(S_a\psi \wedge S_b\neg\psi)$、$S_aS_b\varphi$ 等表达式，其对应公理系统则应是 **ICST4** 上的扩展。我们将纯秘密逻辑的多主体扩张与 **S5** 框架下的公理系统留作未来的工作。

4 结语

从分析“秘密”概念的不同层次理解入手，本文引出了“独知”概念，并在知识逻辑的基础上定义了独知逻辑。我们使用 $O_a\varphi$ 来表示 φ 为主体 a 所独知，从而可以用 $K_aO_a\varphi$ 和 $K_aO_aK_a\varphi$ 来分别表示“φ 是 a 的秘密”与“$K_a\varphi$ 是 a 的秘密”。并论证了独知逻辑语言 $\mathcal{L}_{KO}$ 比纯秘密逻辑语言 $\mathcal{L}_S$ 有着更强的表达力，它可以用于研究多主体系统（尤其是无穷主体系统）下的含有知识模态的秘密逻辑（$\mathcal{L}_{SK}$）。在无穷主体集下，我们给出了独知逻辑可靠且强完全的无穷公理系统（系统中包含一条无穷规则 DeR）。类似的，在无穷主体集下，秘密逻辑 $\mathcal{L}_{SK}$ 与独知逻辑一样，也是非紧致的，因而独知逻辑的无穷证明系统可作为 $\mathcal{L}_{SK}$ 的无穷公理

[20] 从 **IC** 可推出 K 公理与 RE 规则（见 [16]）。

系统的参照。有穷主体集下，独知逻辑可归约为知识逻辑。无穷主体集下，独知逻辑的有穷公理系统及其完全性问题也是一个有趣的议题，除了 [15] 给出的随机命题网络宣告逻辑（APNAL）的无穷公理系统，[3] 也给出了随机公开宣告逻辑（APAL）的无穷公理系统，但关于 APAL 这类逻辑的有穷公理系统还有待研究。[21]

另外，与纯秘密逻辑类似，（不包含知识算子）的纯独知逻辑的公理系统也有待研究，我们可以参考对二元关系“打包”的标准模型来讨论纯独知逻辑的典范模型。但这一方法并不是可直接套用的，现有的标准模型中 $O(w,u,v)$ 是形如 wR_au 且 uR_bv 的复合，与秘密模态的语言定义密切相关。但独知模态的语义要求我们关注的是形如 wR_au 与 wR_bv 上的关系，现有标准模型的定义并不符合语义要求。值得注意的还有，纯独知逻辑与纯秘密逻辑在公理系统上有何异同也是有待研究的议题。在纯独知逻辑系统中，形如 C 公理 $(O_a\varphi \wedge O_a\psi) \to O_a(\varphi \wedge \psi)$、S 公理 $O_a\top \leftrightarrow O_a\bot$ 都是有效的；I 规则：从“$\varphi \to \psi, \psi \to \chi$”推出“$(O_a\varphi \wedge O_a\chi) \to O_a\psi$”则是保有效的。形如单调性规则：如从 $\varphi \to \psi$ 推出 $O_a\varphi \to O_a\psi$ 不是保有效的，C 公理的逆命题 $O_a(\varphi \wedge \psi) \to (O_a\varphi \wedge O_a\psi)$ 也不是有效式等，这些都与纯秘密逻辑的性质是一样的。纯独知逻辑的公理系统及其与纯秘密逻辑系统间的异同有待进一步研究。

本文的另一个主要工作是推进了纯秘密逻辑公理系统上的扩展。我们给出了单主体纯秘密逻辑的公理系统 **ICST4**，使用“标准模型”与“带标签的典范模型”证明了其完全性，并通过模型翻译，证明了 **ICST4** 在 R_a 自反和 R_a 传递的框架下是强完全的。这些技术方法并不是对 [16] 中方法的直接套用，我们重新定义了标准模型上的“典范关系”，构造了能够扩展为“典范标准模型”的预模型，完成了有穷公理系统 **ICST4** 完全性的证明。这样使用“标签”扩展典范世界、构造标准模型“打包”可及关系以及给出标准模型与克里普克模型间的翻译等技术方法对“多主体关系互动”的认知模态公理系统证明有着一定的启发意义。进一步，我们还论证了 **ICST4** 系统的扩展 **ICST45** 是不可靠的。是否还存在对 **ICST4** 可靠的真扩展、**ICST4** 是否在等价框架上也是完全的、纯秘密逻辑系统的多主体扩展等问题则有待进一步研究。

参考文献

[1] T. Ågotnes and M. Walicki, 2005, “Strongly complete axiomatizations of ‘knowing at most’ in syntactic structures”, *International Workshop on Computational Logic in Multi-Agent Systems*, pp. 57–76.

[21] [13] 将宣告命题限制在布尔公式上，介绍了布尔公式下随机公开宣告逻辑（BAPAL）的有穷公理系统。

[2] A. Aldini, D. Fazio, P. Graziani, R. Mascella and M. Tagliaferri, 2025, “A logical perspective on intending to keep a true secret”, *Journal of Logic and Computation*, **35(5)**: exaf028.

[3] P. Balbiani and H. van Ditmarsch, 2015, “A simple proof of the completeness of APAL”, *Studies in Logic*, **8(1)**: 65–78.

[4] W. Craig, 1957, “Three uses of the Herbrand-Gentzen theorem in relating model theory and proof theory”, *The Journal of Symbolic Logic*, **22(3)**: 269–285.

[5] H. van Ditmarsch, W. van der Hoek and B. Kooi, 2007, *Dynamic Epistemic Logic*, **Vol. 337**, Berlin: Springer.

[6] J. Fan, 2025, “Radical ignorance and the Dunning–Kruger effect: An improved account of the logic involved”, *Synthese*, **205(6)**: 1–30.

[7] J. Fan, Y. Wang and H. van Ditmarsch, 2015, “Contingency and knowing whether”, *The Review of Symbolic Logic*, **8(1)**: 75–107.

[8] L. Humberstone, 2012, “Minimally congruential contexts: Observations and questions on embedding E in K”, *Notre Dame Journal of Formal Logic*, **53(4)**: 581–598.

[9] S. M. More and P. Naumov, 2010, “An independence relation for sets of secrets”, *Studia Logica*, **94(1)**: 73–85.

[10] S. M. More and P. Naumov, 2011, “Logic of secrets in collaboration networks”, *Annals of Pure and Applied Logic*, **162(12)**: 959–969.

[11] P. Blackburn, M. de Rijke and Y. Venema, 2001, *Modal Logic*, **Vol. 53**, Cambridge: Cambridge University Press.

[12] F. Van De Putte and P. McNamara, 2022, “Neighbourhood canonicity for EK, ECK, and relatives: A constructive proof”, *The Review of Symbolic Logic*, **15(3)**: 607–623.

[13] H. van Ditmarsch and T. French, 2022, “Quantifying over boolean announcements”, *Logical Methods in Computer Science*, **18(1)**: 1–22.

[14] H. van Ditmarsch, W. van der Hoek and L. B. Kuijer, 2020, “The logic of gossiping”, *Artificial Intelligence*, **286(2020)**: 103306.

[15] Z. Xiong and T. Ågotnes, 2020, “Arbitrary propositional network announcement logic”, in M. A. Martins and I. Sedlár(eds.), *Dynamic Logic. New Trends and Applications*, pp. 277–293, Cham: Springer International Publishing.

[16] Z. Xiong and T. Ågotnes, 2023, “The logic of secrets and the interpolation rule”, *Annals of Mathematics and Artificial Intelligence*, **91(4)**: 375–407.

[17] 李延军，“动态逻辑 AUL 中的秘密宣告”，逻辑学研究，2020 年第 6 期，第 63–88 页。

[18] 熊作军，张玉志，“关于‘秘密’的逻辑语义研究”，湖南科技大学学报（社会科学版），2021 年第 3 期，第 27–38 页。

[19] 张玉志，社会网络中信息流动与主体完美回忆研究，博士论文，西南大学，2020 年。

（责任编辑：映之）

On the Logic of Exclusive Knowing and Secrets

Zuojun Xiong

Abstract

"Exclusive knowing" refers to what is known only by a single individual, serving as a necessary condition for that individual to know a proposition secretly. This paper discusses the modality of "exclusive knowing" and its axiomatisation based on epistemic logic, and further extends the secret logic by constructing an *exclusive knowing logic* based on the **S5** system and a *pure secret logic* based on the **S4** system. Regarding exclusive knowing logic, its non-compactness under an "infinite set of agents" is demonstrated, and a sound and *strongly* complete "infinitary axiomatisation" is provided. In terms of secret logic, building upon the pure secret logic (finitary) axiomatisation **ICST** (without the knowledge operator) from a single-agent perspective, this paper extends it with the positive introspection axiom (axiom 4), resulting in the **ICST4** system. The completeness of this system over reflexive and transitive Kripke models is proven using *canonical standard models* and *translations*. Finally, the paper discusses potential extensions related to exclusive knowing logic and secret logic.

Zuojun Xiong Institute of Logic and Intelligence, Southwest University
zuojunxiong@swu.edu.cn