第 38 卷　第 2 期
2023 年 4 月

天津科技大学学报
Journal of Tianjin University of Science & Technology

Vol. 38　No. 2
Apr. 2023

DOI:10.13364/j.issn.1672-6510.20220249

标准当前状态不透明性与强当前状态不透明性的归约

魏佳唯，赵　骥，陈晓艳，韩晓光
（天津科技大学电子信息与自动化学院，天津 300222）

摘　要：不透明性是信息流安全中的一种重要属性，它表征了系统对入侵者保密的能力.在离散事件系统中，标准当前状态不透明性刻画的是入侵者无法根据当前的输出观测序列确定系统是否达到秘密状态. 强当前状态不透明性刻画的是对每一个到达秘密状态的运行，存在一个观测等价的非秘密运行与之对应. 显然，强当前状态不透明性比标准当前状态不透明性具有更强的隐秘性. 针对标准当前状态不透明性与强当前状态不透明性之间的归约问题，提出一种新的转换方法，即在原系统基础上添加一些新的状态及相关跃迁，分别构造两个新的系统，证明了原系统是标准当前状态不透明的（强当前状态不透明的），当且仅当新系统是强当前状态不透明的（标准当前状态不透明的）.

关键词：离散事件系统；标准当前状态不透明性；强当前状态不透明性；归约
中图分类号：TP273　　**文献标志码**：A　　**文章编号**：1672-6510（2023）02-0070-05

Reduction Between Standards and Strong Current-State Opacity

WEI Jiawei，ZHAO Ji，CHEN Xiaoyan，HAN Xiaoguang
（College of Electronic Information and Automation，Tianjin University of Science & Technology，
Tianjin 300222，China）

Abstract：Opacity，as an important property in information-flow security，characterizes the ability of a system to keep some secret information from an intruder. In discrete-event systems，standard current-state opacity characterizes that an intruder cannot determine for sure whether a system has reached a secret state based on the current sequence of output observations. Strong current-state opacity describes that for each run of a system ending at secret state，there exists a non-secret run whose observation is the same as that of the previous run. Obviously，it has higher-level confidentiality than the standard current-state opacity. For the reduction problem between standard and strong current-state opacity，a new conversion method is proposed in this article，that is，two new systems are constructed respectively based on the original system by adding some new states and related transitions. It is proved that the original system is standard current-state opacity（resp.，strong current-state opacity）if and only if the new system is strong current-state opacity（resp.，standard current-state opacity）.

Key words：discrete-event system；standard current-state opacity；strong current-state opacity；reduction

线上服务和网络通信的发展引发了诸多安全和隐私问题. 这要求实际系统在运行过程中具有保护秘密信息的能力. 本文研究了基于有限状态自动机模型的离散事件系统（DES）不透明性的归约问题. 不透明性[1]表征系统的秘密行为对潜在的恶意入侵者是否具有模糊性. 换句话说，如果对系统的每个秘密行为存在一个观测等价的非秘密行为，则系统是不透明的. 不透明性概念最早出现在计算机科学文献[2]中，用于分析加密协议. 此后，在离散事件系统的架构下，科研人员提出不同类型的不透明性概念，包括标准当前状态不透明性[3]、标准初始状态不透明性[4]、标准 K 步不透明性[5]、标准无限步不透明性[6]及基于语言的不透明性[7-8]. 特别地，标准当前状态不透明性描述的是入侵者永远无法确定系统当前是否处于秘密状态.

标准状态不透明性在实际应用中存在一定的局

收稿日期：2022–11–05；**修回日期**：2022–12–29
基金项目：国家自然科学基金资助项目（61903274）
作者简介：魏佳唯（1998—），女，黑龙江海林人，硕士研究生；**通信作者**：韩晓光，副教授，hxg-allen@163.com

限性. 标准状态不透明性无法捕获这样一种情形：入侵者永远无法根据它的观察确定系统是否通过了秘密状态. 即使系统在标准意义上是“不透明的”，入侵者也可能确定系统一定通过了某个秘密状态. 为此，Falcone 等[9]提出了强 K 步不透明性概念，强 K 步不透明性捕获的是在最后 K 观测步长内入侵者无法推断系统是否访问了秘密状态. 后来，Ma 等[10]将强 K 步不透明性概念扩展到强无限步不透明性. 强无限步不透明性是标准无限步不透明性的强版本. Han 等[11]提出了强当前状态不透明性和强初始状态不透明性的概念，它们分别是标准当前状态不透明性和标准初始状态不透明性的强版本. 此外，为了有效地验证这 4 种强版本不透明性，作者提出了两个新的并发合成信息结构，详见文献[11–12]. Cassez 等[13]设计了基于语言的不透明性转换为标准当前状态不透明性的多项式时间算法. Wu 等[14]证明了标准当前状态不透明性、初始和最终状态不透明性及基于语言的不透明性在多项式时间内可以相互转换，并进一步设计了将标准初始状态不透明性转换为基于语言的不透明性及初始和最终状态不透明性的算法，以及对前缀闭包语言，给出了将基于语言的不透明性转换为标准初始状态不透明性的转换方法. Balun 等[15]扩展了这些结果，证明了上述所有标准不透明性概念之间皆可相互转换. 归约从结构的角度更深入地反映了不透明性概念之间的差异. 同时，归约也提供了一种方法论：针对存在多项式时间转换算法的各种不透明性概念，人们只需要讨论其中一个不透明性概念的验证和强化问题即可. 至今，标准不透明性与强不透明性之间的归约问题尚未被研究.

为此，本文研究标准当前状态不透明性与强当前状态不透明性之间的转换. 受文献[15]的启发，本文提出一种标准当前状态不透明性和强当前状态不透明性之间的转换方法. 即基于给定的原系统分别构造两个新系统，使其满足：(1) 原系统是标准当前状态不透明的，当且仅当新系统是强当前状态不透明的；(2) 原系统是强当前状态不透明的，当且仅当新系统是标准当前状态不透明的. 该转换方法是在多项式时间内可计算的. 最后，实例说明了本文所设计转换方法的可行性和有效性.

1　预备知识

1.1　系统模型

本文将一个离散事件系统（下文简称为系统）建模为非确定型有限状态自动机

$$G=(X,\Sigma,\delta,X_0)$$

其中：X 是有限状态集，Σ 是有限事件集，$X_0\subseteq X$ 是初始状态集，$\delta: X\times\Sigma\to 2^X$ 是跃迁函数，描述了系统动态行为：给定状态 $x,y\in X$ 和一个事件 $\sigma\in\Sigma$，$y\in\delta(x,\sigma)$ 意味着存在一个由 σ 标记的从 x 到 y 的跃迁. 跃迁函数 δ 可通过递归方式扩展为 $\delta: X\times\Sigma^*\to 2^X$，其中 Σ^* 表示 Σ 的克林尼闭包，即由 Σ 中事件构成的所有有限序列（包括空序列）的集合（详见文献[16]）. $L(G,x)$ 表示系统 G 从状态 x 出发生成的语言，即 $L(G,x)=\{s\in\Sigma^*\mid\delta(x,s)\neq\varnothing\}$. 因此，系统 G 生成的语言为 $L(G)=\bigcup_{x_0\in X_0}L(G,x_0)$. 不失一般性，假设系统 G 是可接近的，即它的所有状态皆是从状态集 X_0 可达的.

按照惯例，假设入侵者只能看到系统的局部行为. 因此，事件集 Σ 被划分为可观事件集 $\Sigma_{\rm o}$ 和不可观事件集 $\Sigma_{\rm uo}$，即 $\Sigma_{\rm o}\cap\Sigma_{\rm uo}=\varnothing$ 且 $\Sigma_{\rm o}\cup\Sigma_{\rm uo}=\Sigma$. 自然投影 $P:\Sigma^*\to\Sigma_{\rm o}^*$ 递归定义为

$$P(\epsilon)=\epsilon,\ P(s\sigma)=\begin{cases}P(s)\sigma, & \text{如果}\sigma\in\Sigma_{\rm o}\\ P(s), & \text{如果}\sigma\in\Sigma_{\rm uo}\end{cases}$$

其中 $s\in\Sigma^*$.

给定系统 $G=(X,\Sigma,\delta,X_0)$，$X_{\rm S}\subseteq X$ 表示秘密状态集，$X_{\rm NS}\subseteq X$ 表示非秘密状态集. 假设 $s=s_1s_2\cdots s_n\in\Sigma^*$，$x_0\in X_0, x_i\in X, i=1,2,\cdots,n$. 如果 $x_{k+1}\in\delta(x_k,s_{k+1}),\ 0\leqslant k\leqslant n-1$，称 $x_0\xrightarrow{s_1}x_1\xrightarrow{s_2}x_2\xrightarrow{s_3}\cdots\xrightarrow{s_n}x_n$ 为系统 G 在 s 下从 x_0 到 x_n 的一个运行. 当未指定状态 $x_1,x_2,\cdots,x_{n-1}$（或 $x_1,x_2,\cdots,x_n$）时，简记为 $x_0\xrightarrow{s}x_n$（或 $x_0\xrightarrow{s}$）. 值得注意的是，由于系统 G 是不确定的有限状态自动机，这意味着 $x_0\xrightarrow{s}x_n$ 可能表示多个运行. 在本文中，$x_0\xrightarrow{s}x_n$ 始终表示一个运行. 特别地，如果 $x_i\notin X_{\rm S}$，$i=0,1,2,\cdots,n$，称 $x_0\xrightarrow{s_1}x_1\xrightarrow{s_2}x_2\xrightarrow{s_3}\cdots\xrightarrow{s_n}x_n$ 为一个非秘密运行.

1.2　标准当前状态不透明性与强当前状态不透明性

在这一小节，分别回顾标准当前状态不透明性和强当前状态不透明性的形式化定义.

定义 1（标准当前状态不透明性[3]）给定系统 $G=(X,\Sigma,\delta,X_0)$，投影映射 $P:\Sigma^*\to\Sigma_{\rm o}^*$，可观事件集 $\Sigma_{\rm o}$，秘密状态集 $X_{\rm S}\subseteq X$. 如果对所有满足条件 $\delta(x_0,s)\cap X_{\rm S}\neq\varnothing$ 的 $x_0\in X_0$ 和 $s\in L(G,x_0)$，都有 $(\exists x_0'\in X_0)(\exists t\in L(G,x_0'))[\delta(x_0',t)\cap X_{\rm NS}\neq\varnothing\wedge P(t)=P(s)]$，则称系统 G 是标准当前状态不透明的.

定义 2（强当前状态不透明性[11]）给定系统

$G=(X,\Sigma,\delta,X_0)$，投影映射 $P:\Sigma^*\to\Sigma_o^*$，可观事件集 Σ_o，秘密状态集 $X_S\subseteq X$．如果对所有满足条件 $\delta(x_0,s)\cap X_S\neq\varnothing$ 的 $x_0\in X_0$ 和 $s\in L(G,x_0)$，存在一个非秘密运行 $x_0'\xrightarrow{t}x$，使得 $P(t)=P(s)$ 成立，其中 $x_0'\in X_0$，$x\in X$，则称系统 G 是强当前状态不透明的.

例 1 考虑图 1 所示系统 G_1，其中 $X_S=\{x_2\}$，$\Sigma_o=\{a,b\}$．对字符串 $s=a:\delta(x_1,s)=\{x_2\}$，存在一个投影与之等价的字符串 $t=au$，使得 $\delta(x_1,t)=\{x_3\}$，根据定义 1，系统 G_1 是标准当前状态不透明的. 但是，系统 G_1 不是强当前状态不透明的. 因为与字符串 $s=a$ 观测等价的所有字符串皆到达(或经过)秘密状态 x_2.

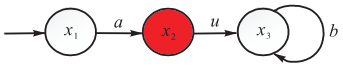

图 1　系统 G_1：$X_S=\{x_2\}$，$\Sigma_o=\{a,b\}$
Fig. 1　System G_1 with $X_S=\{x_2\}$ and $\Sigma_o=\{a,b\}$

例 2 考虑图 2 所示系统 G_2，其中 $X_S=\{x_5\}$，$\Sigma_o=\{a,b\}$．对字符串 $s=ab:\delta(x_1,s)=\{x_5\}$，存在一个投影与之等价的字符串 $t=aub$，使得 $x_1\xrightarrow{t}x_3$ 是一个非秘密运行. 根据定义 2，系统 G_2 是强当前状态不透明的.

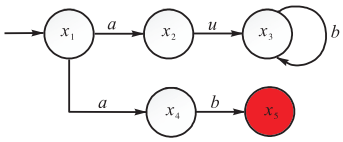

图 2　系统 G_2：$X_S=\{x_5\}$，$\Sigma_o=\{a,b\}$
Fig. 2　System G_2 with $X_S=\{x_5\}$ and $\Sigma_o=\{a,b\}$

2　标准与强当前状态不透明性之间的归约

2.1　标准当前状态不透明性到强当前状态不透明性的转换

在这一小节，讨论系统从标准当前状态不透明性到强当前状态不透明性的转换. 具体如下：考虑系统 $G_{CSO}=(X,\Sigma,\delta,X_0)$，秘密状态集 $X_S\subseteq X$，非秘密状态集 $X_{NS}\subseteq X$．构造一个新系统 $G_{SCSO}=(X',\Sigma',\delta',X_0')$，其中 $X'=X_S'\cup X_{NS}'\cup X_{S\text{-}NS}'$，这里，新添加的状态集 $X_{S\text{-}NS}'$ 中的状态既不是秘密的也不是非秘密的，X_S' 和 X_{NS}' 的解释如下：$X_{NS}'=X_{NS}$，对所有的 $x_S\in X_S$，将 x_S 拆分为 x_S^- 和 x_S^+，其中 $x_S^-\in X_S'$，$x_S^+\in X_{S\text{-}NS}'$（原跃迁关系保持不变）.

备注 1 系统 G_{CSO} 有计算复杂度 $\mathcal{O}(|\Sigma||X|^2)$．因此，构造系统 G_{SCSO} 的计算复杂度为 $\mathcal{O}(4|\Sigma||X|^2)$．其中 $|\Sigma|$ 和 $|X|$ 分别表示系统 G_{CSO} 的事件数和状态数.

定理 1 系统 G_{CSO} 是标准当前状态不透明的，当且仅当系统 G_{SCSO} 是强当前状态不透明的.

证明 必要性：设系统 G_{CSO} 是标准当前状态不透明的. 据定义 1，对任意 $x_0\in X_0$，$s\in L(G_{CSO},\ x_0)$ 使得 $\delta(x_0,s)\cap X_S\neq\varnothing$，存在一个运行 $x_0'\xrightarrow{t}x_{NS}$，其中 $x_0'\in X_0,x_{NS}\in X_{NS},P(t)=P(s)$．为两种情况：

(1) 若 $x_0'\xrightarrow{t}x_{NS}$ 本身是一个非秘密运行，根据定义 2，系统 G_{SCSO} 是强当前状态不透明的；

(2) 若 $x_0'\xrightarrow{t}x_{NS}$ 是一个秘密运行，根据系统 G_{SCSO} 的构造，$x_0'\xrightarrow{t}x_{NS}$ 经过的所有秘密状态皆被拆分成两部分. 不妨设 $x_0'\xrightarrow{t}x_{NS}$ 经过 $k(k\geqslant 1)$ 个秘密状态，表示为 $x_{S1},x_{S2},\cdots,x_{Sk}$．$x_{Si}$ 被拆分为 x_{Si}^- 和 x_{Si}^+，其中 $x_{Si}^-\in X_S',x_{Si}^+\in X_{S\text{-}NS}',i=1,2,\cdots,k$．这样，在系统 G_{SCSO} 中存在一个非秘密运行 $x_0'\xrightarrow{t_1}x_{S1}^+\xrightarrow{t_2}x_{S2}^+\to\cdots\to x_{Sk}^+\xrightarrow{t_{k+1}}x_{NS}$，其中 $t=t_1t_2\cdots t_{k+1}$，$t_j\in(\Sigma')^*$，$j=1,2,\cdots,k+1$. 根据定义2，系统 G_{SCSO} 是强当前状态不透明的.

充分性：采用反证法，若系统 G_{CSO} 不是标准当前状态不透明的. 则在系统 G_{CSO} 中存在一个运行 $x_0\xrightarrow{s}x_S,x_S\in X_S$，使得对任意运行 $x_0'\xrightarrow[P(t)=P(s)]{t}x$，必有 $x\in X_S$. 根据系统 G_{SCSO} 的构造，原系统 G_{CSO} 的跃迁关系在系统 G_{SCSO} 中保持不变. 因此，在系统 G_{SCSO} 中存在运行 $x_0\xrightarrow{s}x_S^-$，且对任意运行 $x_0'\xrightarrow[P(t)=P(s)]{t}x$，必有 $x\in X_S'$ 或 $x\in X_{S\text{-}NS}'$．根据定义 2，系统 G_{SCSO} 不是强当前状态不透明的.

例 3 再次考虑图 1 所示系统 $G_1=(X,\Sigma,\delta,X_0)$，其中 $X_S=\{x_2\}$，$\Sigma_o=\{a,b\}$，由例 1 可知系统 G_1 是标准当前状态不透明的. 从系统 G_1，构造一个新的系统 $G_1'=(X',\Sigma',\delta',X_0')$，如图 3 所示．对字符串 $s=a:\delta'(x_1,s)=\{x_2^-\}$，存在一个投影与之等价的字符串 $t=au$，使得 $x_1\xrightarrow{a}x_2^+\xrightarrow{u}x_3$ 是一个非秘密运行. 根据定义 2，系统 G_1' 是强当前状态不透明的.

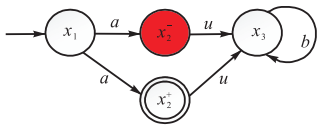

图 3　系统 G_1'：$X_S'=\{x_2^-\}$，$\Sigma_o'=\{a,b\}$
Fig. 3　System G_1' with $X_S'=\{x_2^-\}$ and $\Sigma_o'=\{a,b\}$

2.2　强当前状态不透明性到标准当前状态不透明性的转换

在这一小节，讨论系统从强当前状态不透明性到标准当前状态不透明性的转换. 具体如下：考虑系统

$G_{SCSO}=(X,\Sigma,\delta,X_0)$，秘密状态集 $X_S\subseteq X$，非秘密状态集 $X_{NS}\subseteq X$．构造一个新系统 $G_{CSO}=(X',\Sigma',\delta',X_0')$，其中 $X'=X_S'\cup X_{NS}'\cup X_{S\text{-}NS}'$，这里，新添加的状态集 $X_{S\text{-}NS}'$ 中的状态既不是秘密的也不是非秘密的，X_S' 和 X_{NS}' 的解释如下：$X_S'=X_S$，对所有的 $x_{NS}\in X_{NS}$，分为 3 种情况：

(1) 若对任意 $x_0\in X_0$，$x_0\xrightarrow{s}x_{NS}$ 都是一个秘密运行，则令 $x_{NS}\in X_{S\text{-}NS}'$；

(2) 若对任意 $x_0\in X_0$，$x_0\xrightarrow{s}x_{NS}$ 都是一个非秘密运行，则令 $x_{NS}\in X_{NS}'$；

(3) 若对 $x_0,x_0'\in X_0$，$x_0\xrightarrow{s}x_{NS}$ 是一个秘密运行，$x_0'\xrightarrow{s}x_{NS}$ 是一个非秘密运行，则拆分 x_{NS} 为 x_{NS}^+ 和 x_{NS}^-，其中 $x_{NS}^+\in X_{S\text{-}NS}'$，$x_{NS}^-\in X_{NS}'$．因为系统 G_{SCSO} 的跃迁关系在系统 G_{CSO} 中保持不变，则 $x_0\xrightarrow{s}x_{NS}^+$ 是 G_{CSO} 的一个秘密运行，$x_0\xrightarrow{s}x_{NS}^-$ 是 G_{CSO} 的一个非秘密运行．

备注 2 系统 G_{SCSO} 有计算复杂度 $\mathcal{O}(|\Sigma||X|^2)$．因此，构造系统 G_{CSO} 的计算复杂度为 $\mathcal{O}(4|\Sigma||X|^2)$．

定理 2 系统 G_{SCSO} 是强当前状态不透明的，当且仅当系统 G_{CSO} 是标准当前状态不透明的．

证明 必要性：设系统 G_{SCSO} 是强当前状态不透明的．根据定义 2，对任意运行 $x_0\xrightarrow{s}x_S$，$x_S\in X_S$，都存在一个非秘密运行 $x_0'\xrightarrow{t}x$，使得 $P(t)=P(s)$ 成立．根据系统 G_{CSO} 的构造，原系统 G_{SCSO} 的跃迁关系在系统 G_{CSO} 中保持不变．因此，系统 G_{CSO} 中必存在非秘密运行 $x_0'\xrightarrow{t}x$ 或 $x_0'\xrightarrow{t}x^-$．根据定义 1，系统 G_{CSO} 是标准当前状态不透明的．

充分性：采用反证法，若系统 G_{SCSO} 不是强当前状态不透明的．则在系统 G_{SCSO} 中存在一个运行 $x_0\xrightarrow{s}x_S,x_S\in X_S$，使得任意运行 $x_0'\xrightarrow[P(t)=P(s)]{t}x$ 都是秘密运行．有以下两种情况：

(1) 若状态 $x\in X_S$，根据定义 1，系统 G_{CSO} 不是标准当前状态不透明的；

(2) 若状态 $x\in X_{NS}$，分为两种情况：若从任意初始状态出发，到达状态 x 的运行皆为秘密运行，则令 $x\in X_{S\text{-}NS}'$；若从任意初始状态出发，到达状态 x 的运行既有秘密运行又有非秘密运行（注意：所有的非秘密运行投影皆不等于 $P(s)$），则拆分 x 为 x^+ 和 x^-，其中 $x^+\in X_{S\text{-}NS}'$，$x^-\in X_{NS}'$．根据系统 G_{CSO} 的构造，原系统 G_{SCSO} 的跃迁关系在系统 G_{CSO} 中保持不变．因此，系统 G_{CSO} 中存在运行 $x_0'\xrightarrow[P(t)=P(s)]{t}x^+$．

这样，在系统 G_{CSO} 中，对任意 $x_0\in X_0'$，$s\in L(G_{CSO},x_0)$ 使得 $\delta'(x_0,s)\cap X_S'\neq\varnothing$，总是存在一个字符串 t，使得 $\delta'(x_0',t)\in X_S'$ 或 $\delta'(x_0',t)\in X_{S\text{-}NS}'$，即 $\delta'(x_0',t)\cap X_{NS}'=\varnothing$．根据定义 1，系统 G_{CSO} 不是标准当前状态不透明的．

例 4 考虑图 4 所示系统 $G_3=(X,\Sigma,\delta,X_0)$，其中 $X_S=\{x_1,x_2,x_5,x_6\}$，$\Sigma_o=\{a,b\}$．对字符串 $s=uab$：$\delta(x_0,s)=\{x_6\}$，不存在投影与之等价的字符串 $t\in L(G_3)$，使得 $x_0\xrightarrow{t}$ 是一个非秘密运行．根据定义 2，系统 G_3 不是强当前状态不透明的．基于系统 G_3，构造一个新的系统 $G_3'=(X',\Sigma',\delta',X_0')$，如图 5 所示．对字符串 $s=uab:\delta'(x_0,s)=\{x_6\}$，投影与 s 等价的字符串有 $t_1=uab$，$t_2=aub$，$t_3=uaub$．因为 $\delta'(x_0,t_j)\cap X_{NS}'=\varnothing$，$j=1,2,3$，根据定义 1，系统 G_3' 不是标准当前状态不透明的．

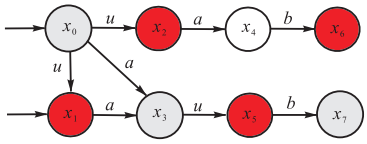

图 4　系统 G_3：$X_S=\{x_1,x_2,x_5,x_6\}$，$\Sigma_o=\{a,b\}$

Fig. 4　System G_3 with $X_S=\{x_1,x_2,x_5,x_6\}$ and $\Sigma_o=\{a,b\}$

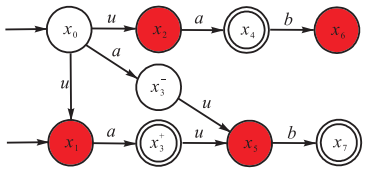

图 5　系统 G_3'：$X_S'=\{x_1,x_2,x_5,x_6\}$，$\Sigma_o'=\{a,b\}$

Fig. 5　System G_3' with $X_S'=\{x_1,x_2,x_5,x_6\}$ and $\Sigma_o'=\{a,b\}$

3　结　语

本文研究标准当前状态不透明性与强当前状态不透明性之间的归约问题．为了实现这两种不透明性之间的转换，在原系统基础上，分别构造了两个多项式复杂度的新系统，证明了标准当前状态不透明性与强当前状态不透明性通过这种转换是等价的．未来尝试将本文提出的归约方法扩展到其他不透明性的转换问题中．

参考文献：

[1] LAFORTUNE S, LIN F, HADJICOSTIS C N. On the history of diagnosability and opacity in discrete event systems[J]. Annual reviews in control, 2018, 45: 257–266.

[2] MAZARÉ L. Using unification for opacity properties[R/OL]. (2004–10–28)[2022–10–12]. https://www-verimag.imag.fr/TR/TR-2004-24.pdf.
[3] SABOORI A, HADJICOSTIS C N. Notions of security and opacity in discrete event systems[C]//2007 46th IEEE Conference on Decision and Control. New Orleans: IEEE, 2007: 5056–5061.
[4] SABOORI A, HADJICOSTIS C N. Verification of initial-state opacity in security applications of discrete event systems[J]. Information sciences, 2013, 246: 115–132.
[5] SABOORI A, HADJICOSTIS C N. Verification of *K*-step opacity and analysis of its complexity[J]. IEEE Transactions on automation science and engineering, 2011, 8(3): 549–559.
[6] SABOORI A, HADJICOSTIS C N. Verification of infinite-step opacity and complexity considerations[J]. IEEE Transactions on automatic control, 2011, 57(5): 1265–1269.
[7] BRYANS J W, KOUTNY M, MAZARÉ L, et al. Opacity generalized to transition systems[J]. International journal of information security, 2008, 7(6): 421–435.
[8] LIN F. Opacity of discrete event systems and its applications[J]. Automatica, 2011, 47(3): 496–503.
[9] FALCONE Y, MARCHAND H. Enforcement and validation (at runtime) of various notions of opacity[J]. Discrete event dynamic systems, 2015, 25(4): 531–570.
[10] MA Z Y, YIN X, LI Z W. Verification and enforcement of strong infinite- and *k*-step opacity using state recognizers[J]. Automatica, 2021, 133: 109838.
[11] HAN X G, ZHANG K Z, ZHANG J H, et al. Strong current-state and initial-state opacity of discrete-event systems[J]. Automatica, 2023, 148: 110756.
[12] HAN X G, ZHANG K Z, LI Z W. Verification of strong K-step opacity for discrete-event systems[EB/OL]. (2022–04–10)[2022–10–20]. https://arxiv.org/pdf/2204.04698.pdf.
[13] CASSEZ F, DUBREIL J, MARCHAND H. Synthesis of opaque systems with static and dynamic masks[J]. Formal methods in system design, 2012, 40(1): 88–115.
[14] WU Y C, LAFORTUNE S. Comparative analysis of related notions of opacity in centralized and coordinated architectures[J]. Discrete event dynamic systems, 2013, 23(3): 307–339.
[15] BALUN J, MASOPUST T. Comparing the notions of opacity for discrete-event systems[J]. Discrete event dynamic systems, 2021, 31(4): 553–582.
[16] CASSANDRAS C G, LAFORTUNE S. Introduction to discrete event systems[M]. Boston: Springer, 2008.

责任编辑：周建军

（上接第 27 页）

gens[J]. Naturwissenschaften, 1985, 72: 212–213.
[29] BIASINI M, BIENERT S, WATERHOUSE A, et al. SWISS-MODEL: modelling protein tertiary and quarternary structure using evolutionary information[J]. Nucleic acids research, 2014, 42(1): 252–258.
[30] 郑礼娜. 虾类过敏原的活性分析及其抗原表位的研究[D]. 青岛：中国海洋大学，2011.

责任编辑：郎婧