

基于进化理论的可信计算环境实现

周毅¹, 贾佳², 廖军², 肖征荣²

(1. 中国软件评测中心, 北京 100042;

2. 中国联通研究院, 北京 100032)

摘要:文中对可信计算环境进行分析,提出了可信计算环境的公理系统。在综合研究了生物科学中的进化理论后给出了可信计算环境的进化方式:提出了基于用进废退的信任输入模型、基于人的选择的信任收敛模型、基于点断平衡论的信任模型;实现了基于进化理论的可信计算环境。仿真结果表明,可信计算环境的进化为可信计算的发展提供了理论依据,可以使可信计算环境适应变化的输入,并且收敛其信任值,对所有用户进行公正处理,进而高效率低代价就可以构建可信计算环境。

关键词:可信计算;可信计算环境;进化理论

中图分类号:TP309

文献标识码:A

文章编号:1673-629X(2014)07-0099-04

doi:10.3969/j.issn.1673-629X.2014.07.025

Implementation of Trusted Computing Environment Based on Evolutionary Theory

ZHOU Yi¹, JIA Jia², LIAO Jun², XIAO Zheng-rong²

(1. China Software Testing Center, Beijing 100042, China;

2. China Unicom Research Institute, Beijing 100032, China)

Abstract: Analyze the trusted computing environment, and propose an axiom system of trusted computing environment. After the comprehensive study of the theory of evolution in the biological sciences, give the evolution formula of trusted computing environment, including an input trust model based on use and disuse theory, a convergence trust model based on people's choice, and a trust model based on the theory of punctuated equilibrium. Implement the trusted computing environment based on evolutionary theory. The simulation shows that the evolution of trusted computing environment provides a theoretical basis for the development of trusted computing, enables it to adapt to changing and even unknown input, obtaining the convergence of the trust value of trusted computing environment and making it fair for all users. Also, the evolution of trusted computing environment implements trusted computing with a smaller cost.

Key words: trusted computing; trusted computing environment; evolutionary theory

1 研究背景及重要意义

可信计算环境进化的特点使得人应该决定可信计算外部环境。可信计算可以为信息系统提供一个安全的工作环境,制定一套可以执行特殊行为的安全规则^[1]。

目前,计算机系统已经不仅仅拥有最初单一的计算功能,其功能已经渗入到与人类生活息息相关的各个领域,人类所要求的承载人类生活功能的计算系统日渐完善,人类对其依赖与日俱增^[2]。

研究可信计算模型就是为了用较小的代价高效

率,高安全性达到期望值^[3],而进化可信计算环境可以收敛其信任值,对所有用户进行公正处理,进而高效率低代价构建可信计算环境。

2 可信计算环境

以TPM为核心的可信计算环境研究方法是现有的方式^[4]。信任机制可以通过可信存储、可信报告以及可信度量来完成。

可信存储:TPM运用证明能力对数据进行密封存储,TPM基于硬件特点保证存储数据的机密性及完整

性^[5]。

可信报告:可信报告机制可以用来作为验证平台是否可信的依据^[6]。获得 TPM 中的存储度量日志和度量信息可以通过报告机制,若度量信息与预期要求符合,则该平台是可信的,否则该平台被认为是非可信状态。

可信度量:建立可信串时,对于符合要求的需要转移其控制权的前一环节可信串,在控制权转移前均需要对该可信串进行必要的度量^[7]。只有度量值与先前保存的度量值预期值一样,才可转移其控制权。TCG 中规定运用摘要计算成为可信度量的方式^[8],预期值作为预期摘要值,可以成为衡量该实体是否是“预期方式达到预期目标”的依据^[9]。通过这种方式的可信度量,信任把可信根传递至操作系统,从而建立可信的操作系统环境,再从操作系统传递至应用系统,建立可信应用环境,最终从应用传递至网络,建立可信网络环境^[10]。

远程证明:可以与本地系统进行交互,从而向远端服务者提供系统当前软件环境状态,进而使得服务提供者获得可信服务。远程证明是以可信报告机制与可信度量为基础而实现的^[11]。

可信计算环境(Trusted Computing Environment, TCE)研究的内容包括:可信终端、终端可信应用、可信网络连接、可信网络服务器、可信交易以及可信评测方法和管理方法等^[12]。可信计算环境作为研究对象实体时是指图 1 中的虚线部分的内容,包括可信终端、终端可信应用、可信网络连接、可信网络服务器、可信交易。可信计算实体可以代表整个可信计算环境,也可以是可信计算环境的一部分^[13]。

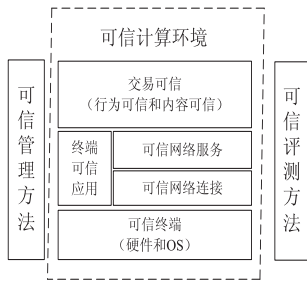


图 1 可信计算环境实体

3 进化理论

生物进化思想经历了最早期的萌芽状态,然后从自然选择学说以及现代综合理论发展至新达尔文主义和分子进化中性学说及点断平衡论^[14]。随着生物学各个分支学科的研究不断深入,其研究对象在各个方面拓展、渗透、交叉最终形成了以遗传为基础的比较基因学以及进化发育生物学^[15]。

1)用进废退学说。

拉马克发表的《动物哲学》阐述了其生物进化思想。其根据生物具有的变异特点,认为自然界的生物是以进化为基础,并且其进化过程是不间断且较缓慢的。其理论包括对生物最具影响力的方面是环境、生物进化具有方向性遗传性以及遵循用进废退原则。

2)自然选择学说。

达尔文的《物种起源》阐述了以遗传为基础的进化学说。其理论包括生物进化的初始状态是可追溯的,生物进化是渐变过程并遵循适者生存原则。

3)新达尔文主义学说。

新达尔文主义学说阐述了基因是遗传物质的基本单位,重点用基因质变、突变以及自然界长期选择的结果来说明生物如何进化。用这种理论可以弥补达尔文主义学说的部分缺陷。

4)现代综合学说。

该学说又称为现代的达尔文主义学说,该学说与新达尔文主义主导的基因论融合,论证了群体遗传学和其他分支学科的融合与发展。

5)中性学说。

中性学说阐述了基因突变是不受自然控制的,而是通过基因突变及漂变遗传使得基因频率最后发生改变而衍变为新生物种群。其中物种进化的速率根本是取决于氨基酸及蛋白质的替换速率。

6)点断平衡理论及新灾变理论。

该理论主要阐述了生物进化并不是只有渐变这一种方式,而是一种非线性交替过程。同时,深入研究了演化过程中出现的种群事件及瞬间事件均是由种系的前进演化来推进的^[16-17]。

4 基于进化理论的可信计算环境实现

4.1 公理系统

可信计算环境的信任模型是基于人的目的一般性认同为基础的。

公理 1:信任托付预期为一个集合 $INTENTION = \{in_i\}, 1 \leq i \leq n$; $INTENTION$ 中的元素总是在不断的变化中,包括新的元素产生,已有元素的变化或者消亡。

公理 2:对于一个确定的可信计算环境的信任托付的预期集合 $INTENTION$,可信计算环境信任损失总是被期望更小。

公理 3:对于可信计算环境的所有信任主体而言可信计算环境应当越来越公正。

4.2 用进废退可信模型

定理 1:用进废退可信模型。

集合 $INTENTION = \{in_i\}, 1 \leq i \leq n$;其定义为可信计算环境下的信任托付预期;

集合 **RULE** 定义为可信计算环境下信任托付预期的法定权利义务关系;

集合 **MORAL** 定义为可信计算环境下信任托付预期的道德权利义务关系;

集合 **NATURE** 定义为可信计算环境下信任托付预期的自然权利义务关系;

$\text{NATURE} \subset \text{INTENTION}$, $\text{RULE} \subset \text{INTENTION}$, $\text{MORAL} \subset \text{INTENTION}$;

$\text{RULE} \cup \text{MORAL} \cup \text{NATURE} = \text{INTENTION}$;

Sum 是信任主体的个数;

信任托付预期为 in_i 的信任主体个数为 sum_{in_i} ;

信任预期 in_i 其利用率表示为 $\text{use}_{\text{in}_i} = \frac{\text{sum}_{\text{in}_i}}{\text{sum}}$;

当 $\text{use}_{\text{in}_i} = 0$ 时,预期退出集合,其他预期产生,并加入新元素。

use_{rule} 定义为法定权利义务关系与道德权利义务关系的边界。 $\text{use}_{\text{moral}}$ 定义为道德权利义务关系与自然权利义务关系预期的边界,有 $0 \leq \text{use}_{\text{rule}} \leq \text{use}_{\text{moral}} \leq 1$;

将 $(0, 1)$ 分为三个区间 $(0, \text{use}_{\text{rule}})$, $(\text{use}_{\text{rule}}, \text{use}_{\text{moral}})$, $(\text{use}_{\text{moral}}, 1)$;

$\text{use}_{\text{in}_i} \in (0, \text{use}_{\text{rule}})$, $\text{in}_i \in \text{RULE}$;

$\text{use}_{\text{in}_i} \in (\text{use}_{\text{rule}}, \text{use}_{\text{moral}})$, $\text{in}_i \in \text{MORAL}$;

$\text{use}_{\text{in}_i} \in (\text{use}_{\text{moral}}, 1)$, $\text{in}_i \in \text{NATURE}$;

信任托付的预期集合是可信计算环境的输入,当且仅当元素使用率是 0 时,其可以退出集合,当且仅当元素的使用率大于 0 时,其可以加入集合。

4.3 可信计算环境下基于人的选择的信任收敛模型

定理 2:可信计算环境信任收敛。

tcp_i 定义为信任实体;

$\text{TCP} = \{ \text{tcp}_i \}$, $1 \leq i \leq n$ 定义为可信计算的实体集合;

tcp_i 信任托付实现是集合 $\text{IMPLEMENT} = \{ \text{im}_i \}$, $1 \leq i \leq n$;

主体 A 对 tcp_i 信任托付实现的信任度表示为集合 $\text{TRUST} = \{ t_i \}$, $1 \leq i \leq n$;

Ξ_i 为对应信任主体 A 对 tcp_i 信任实现运算规则;
 \circ 为对应信任主体 A 对 tcp_i 信任度量运算规则;

对于相同的信任托付预期 in , $\{ \Xi_i \}$, $1 \leq i \leq n$ 为对应 tcp 信任实现运算规则;

$\text{im}_i = \Xi_i(\text{in})$; $t_i = \text{im}_i \circ \text{in} = \Xi_i(\text{in}) \circ \text{in}$;

当有 $t_i = \min \{ t_i \}$ 时, tcp_i 就是层扩张的主体, Ξ_i 就是层扩张的算法。

定理 3:可信度主体偏好的可信度收敛选择。

主体 A 对于可信计算实体 B 的信任托付实现的信任度的属性为集合 $\text{ATTRIBUTE} = \{ \text{at}_k \}$, 且 $\text{at}_k \in R$;

$\text{ORDINAL} = \{ \text{or}_i \} \subseteq \text{ATTRIBUTE}$, $1 \leq i \leq k$, 且其中元素有序;

对于 $\forall \text{at}_k \in \text{ORDINAL}$, 有 $\forall \text{at}_k \in \text{ATTRIBUTE}$;

$\text{or}_1 = (\text{at}_1, \dots, \text{at}_i, \dots, \text{at}_{k-1}, \text{at}_k)$;

$\text{or}_2 = (\text{at}_1, \dots, \text{at}_i, \dots, \text{at}_k, \text{at}_{k-1})$;

当 $t_{\text{at}_1}^1 = t_{\text{at}_1}^2, t_{\text{at}_2}^1 = t_{\text{at}_2}^2, \dots, t_{\text{at}_i}^1 = t_{\text{at}_i}^2, t_{\text{at}_{i-1}}^1 > t_{\text{at}_{i-1}}^2$ 时, $t_{\text{or}_1} > t_{\text{or}_2}$ 。

4.4 可信计算环境下基于点断平衡论的信任模型

定理 4:可信计算环境的三种权力义务模型是不断变化的,同时也在相互转化,当三种模型完全重合时,可信计算环境最公正。

在同一时刻三种权力义务模型的表现形式可能完全不同。在可信计算环境下基于自然权利义务关系的信任模型中的可信计算环境的进化表现为渐变,在可信计算环境下基于法定权利义务关系的信任模型中的可信计算环境的进化表现为突变,而在可信计算环境下基于道德权利义务关系的信任模型中的可信计算环境的进化表现为粗粒度的渐变和多层次的突变。基于点断平衡论说明了可信计算环境的进化过程并不一定一直保持信任收敛,而是突变后阶段性的信任收敛,再突变,再收敛,交替进行。

4.5 可信计算环境实现

基于 TRS 和 NCIC 的可信计算平台,由可信计算平台使用者通过 MMTI 即可确定其信任的预期关系。可信计算模块通过 NCIC 接入可信计算平台中的 TRS 中,进而建立基本可信根、基本可信层、基本可信状态。

四个物理上隔离开的存储空间构成了可信存储根 TRS。其采用的物理隔离方法免去了数据交叉后带来的数据校验开销问题。存储根中基于该理论由统一扩展固件接口 UEFI、应用程序 App (Applications)、操作系统 OS、公众应用程序 PApp (PApp Public Applications)、多主体应用程序 GApp (Groupware Applications) 构成 (见图 2)。

Logical isolation		Logical isolation		Physical isolation	
UEFI	OS	PApp	IApp	DATA	
UEFI	OS	GApp	IGApp		
UEFI	OS	App	App		

图 2 基于进化理论的可信存储根

在 TRS 中,每一种关系的可信根与 NCIC 跟其对应的网络直接连接 (见图 3)。基于进化理论可信存储根与广电网、计算机网络、电信网直接连接;广电网是

以广播方式传输基于法定权利义务关系的可信根。

信任层次	可信存储			可信网络
进	可信UEFI	可信OS	可信应用	广电网
化	可信UEFI	可信OS	可信应用	电信网
理	可信UEFI	可信OS	可信应用	计算机网络
论	可信UEFI	可信OS	可信应用	

图 3 可信环境实现

5 仿真结果

该仿真实验把网络中节点分为两个大类：一部分为正常节点，另一部分为恶意节点；正常节点提供真实的服务及评价，恶意节点则提供虚假的服务及反馈。通过 TTL 来控制查询的规模，通过接收查询节点的消息来查看是否对其应答。其中，发起查询的节点需等待接收响应，其从响应列表之中选取信任值最高的目标节点下载文件，直到监测交易成功或响应宣告失败。

仿真系统的结果（见图 4）说明，基于进化理论的可信计算环境对可信计算整体可信度的提升有极其关键的作用。在基于进化理论的可信计算环境下，通过对点对点的文件共享网络中节点可信度的直接作用，对其下载成功率、成功下载的次数有显著提高，而不成功下载次数有明显下降。在点对点文件共享网络的计算环境下，其下载成功率、成功下载次数以及不成功下载次数均代表可信度。

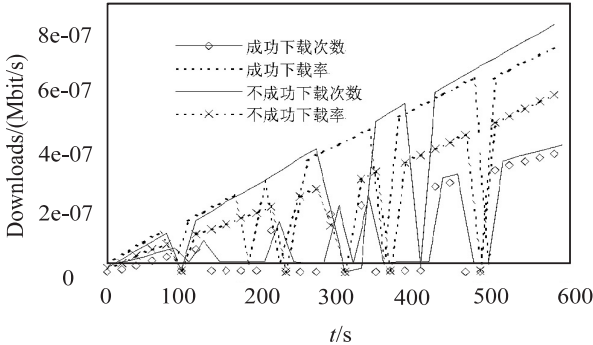


图 4 仿真结果

6 结束语

生物科学中的进化理论为可信计算环境的可信度是否应当一直收敛提出理论依据，进而提出了基于进化理论的可信计算环境。

可信计算环境下用进废退的信任输入模型解决了法定权利义务关系、自然权利义务关系、道德权利义务关系的信任模型这三者之间关系的问题。可信计算环境下基于人的选择的信任模型解决了层扩张的主体确定的问题。可信计算环境下基于点断平衡论的信任模型可以实现公平的开展信任传递。

电信网、计算机网络、广电网与可信存储根直接相连，在物理信道中以广播方式传输可信根。该模型有效地减少了可信终端主动防御而带来的验证开销，进而使得现有计算平台也适用该可信计算环境。同时解决了可信计算环境可信收敛的问题。

下一步的工作将在如何减少可信计算环境的信任损失问题上展开，在文中研究成果的基础之上，针对多信任主体预期语义的分析及信任协商的效率进行重点分析研究，最终使得可信计算环境更加可信。

参考文献：

[1] Guan Shangyuan, Dong Xiaoshe, Wu Weiguo, et al. Trust management and service selection in pervasive computing environments[C]//Proc of international conference on computational intelligence and security workshops. Harbin: IEEE, 2007: 620-623.

[2] Feng Dengguo, Qin Yu. Research on attestation method for trust computing environment[J]. Chinese Journal of Computers, 2008, 31(9): 1640-1652.

[3] TCG TPM Specification Version 1.1b[EB/OL]. [2005-06-20]. https://www.trustedcomputinggroup.org/developers/trusted_platform_module/specification.

[4] Brickell E, Camenisch J, Chen Liqun. Direct anonymous attestation[C]//Proc of the 11th ACM conference on computer and communications security. New York, NY, USA: ACM, 2004: 132-145.

[5] 卿斯汉. 可信计算的研究进展概述[J]. 信息安全, 2008(11): 18-19.

[6] TCG. TCG TNC (Trusted Network Connect) architecture for interoperability ver1.2[EB/OL]. (2007-05-02) [2008-11-24]. http://www.trustedcomputinggroup.org/specs/TNC/TNO_Architecture_V1_2_r4.pdf.

[7] TCG. TCG specification architecture overview ver1.4[EB/OL]. (2007-08-02) [2008-11-24]. https://www.trusted-computinggroup.org/groups/TCG_1_4_Architecture_Overview.pdf.

[8] Brizek J, Khan M, Seifert J P, et al. A platform-level trust-architecture for hand-held devices[C]//Proc of workshop on cryptographic advances in secure hardware. Belgium: [s. n.], 2005.

[9] Eisenbarth T, Güneysu T, Paar C, et al. Reconfigurable trusted computing in hardware[C]//Proceedings of the 2007 ACM workshop on scalable trusted computing. VA, USA: [s. n.], 2007: 15-20.

[10] Dietrich K. An integrated architecture for trusted computing for java enabled embedded devices[C]//Proceedings of the 2007 ACM workshop on scalable trusted computing. VA, USA: [s. n.], 2007: 2-6.

[11] 徐拾义. 可信计算系统设计和分析[M]. 北京: 清华大学出版社, 2005.

In this case, the users do not need to detect the whole object, but prefer detection range delineated by them. Users pull the mouse on a standard template to draw a rectangle, and set it as the ROI^[14-15], thus, system detects the part of the rectangular region only, in order to meet user's needs. In this way, can save a lot of unnecessary consumption of resources and time. However, it does not guarantee the areas out of detection are necessarily qualified. In Figure 4, set the ROI region where the number "8" located in. The result by execute algorithm above on selected region shown in Figure 5. The scratch "1, 2, 3, 0" in this region are detected, and the remaining gray parts are color cast.



Figure 4 Original image of self-selected region

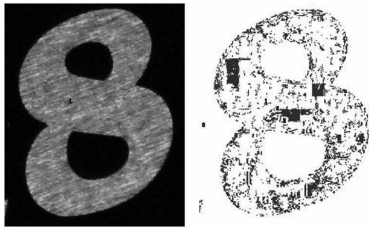


Figure 5 Comparison and result of selected region

3 Conclusion

According to the algorithm proposed, can test out those who do not conform to the specification of products effectively. In the process of actual detection, the value of the threshold is related to the results of the test. So combined with the production specification, determining a suitable threshold is extremely important.

With increasingly preciseness of image acquisition device, as well as improvement of computing capacity, industrial automation and production will become more

prevalent. Combined with machine vision and image processing technology in this field will achieves extensive application prospects.

参考文献:

- [1] 张立凡. 基于机器视觉的图文印刷缺陷检测研究[D]. 北京:北京印刷学院,2010.
- [2] Gonzalez R C. Digital image processing[M]. 3rd ed. London:Prentice Hall,2007.
- [3] 章毓晋. 图像工程[M]. 北京:清华大学出版社,2006.
- [4] Lee S, Chang L M, Skibniewski M. Automated recognition of surface defects using digital color image processing[J]. Automation in Construction, 2006, 15(4):540-549.
- [5] 刘兴, 刘庆祥. 一种彩色图像转换为灰度图像的算法[J]. 现代电子技术, 2007, 30(6):134-135.
- [6] 刘海波. Visual C++数字图像处理技术详解[M]. 北京:机械工业出版社,2010.
- [7] 史迎春, 周献中, 方鹏飞. 综合利用形状和颜色特征的台标识别[J]. 模式识别与人工智能, 2005, 18(2):216-222.
- [8] 曹玉东. 基于融合特征的近似图像检测方法[J]. 计算机技术与发展, 2012, 22(8):103-106.
- [9] Sen D, Pal S K. Gradient histogram; thresholding in a region of interest for edge detection[J]. Image and Vision Computing, 2009, 28(4):677-695.
- [10] 邓秀勤, 熊勇. 用于图像处理的加权中值滤波算法[J]. 计算机技术与发展, 2009, 19(3):46-48.
- [11] Debayle J, Pinoli J. General adaptive neighborhood image processing[J]. Journal of Mathematical Imaging and Vision, 2006, 25(2):245-266.
- [12] 夏平, 刘馨琼, 向学军, 等. 基于形态学梯度的图像边缘检测算法[J]. 计算机技术与发展, 2007, 17(12):107-109.
- [13] Maragos P, Schafer R W, Butt M A. Mathematical morphology and its applications to image and signal processing[M]. Germany:Springer,1996.
- [14] 徐波, 李坤. 基于矩形扩张的 ROI 区域标记算法[J]. 南京信息工程大学学报(自然科学版), 2010, 2(6):573-576.
- [15] 吴志强, 吴乐华, 袁宝峰. 基于分形与小波的图像 ROI 自动提取算法[J]. 计算机应用, 2010, 30(6):1613-1615.


(上接第 102 页)

版社,2006.

- [12] 冯登国, 秦宇. 可信计算环境证明方法研究[J]. 计算机学报, 2008, 31(9):1640-1652.
- [13] 林闯, 田立勤, 王元卓. 可信网络中用户行为可信的研究[J]. 计算机研究与发展, 2008, 45(12):2033-2043.
- [14] 王忠玉. 基于生物进化选择的经济演化理论研究[J]. 经济

评论, 2006(3):145-145.

- [15] 刘海龙. 对生物进化自组织理论具体机制的探讨[J]. 科学技术与辩证法, 2005, 22(6):36-39.
- [16] 余有明, 刘玉树. 进化计算的理论与算法[J]. 计算机应用研究, 2005(9):77-80.
- [17] 李曙新. 哈贝马斯的社会进化理论评析[J]. 社会科学研究, 2004(4):15-18.

作者: 周毅, 贾佳, 廖军, 肖征荣, ZHOU Yi, JIA Jia, LIAO Jun, XIAO Zheng-rong
作者单位: 周毅, ZHOU Yi(中国软件评测中心, 北京, 100042), 贾佳, 廖军, 肖征荣, JIA Jia, LIAO Jun, XIAO Zheng-rong(中国联通研究院, 北京, 100032)
刊名: 计算机技术与发展 
英文刊名: Computer Technology and Development
年, 卷(期): 2014(7)

参考文献(17条)

1. [Guan Shangyuan;Dong Xiaoshe;Wu Weiguo Trust man-agement and service selection in pervasive computing environ-ments](#) 2007

2. [Feng Dengguo;Qin Yu Research on attestation method for trust computing environment](#) 2008(09)

3. [TCG TPM SpecificationVersion1. 1b](#) 2005

4. [Brickell E;Camenisch J;Chen Liqun Direct anonymous attes-tation](#) 2004

5. [卿斯汉 可信计算的研究进展概述](#) 2008(11)

6. [TCG TCG TNC\(Trusted Network Connect\)architecture for interoperability ver1. 2](#) 2008

7. [TCG TCG specification architecture overview ver1. 4](#) 2008

8. [Brizek J;Khan M;Seifert J P A platform-level trust-ar-chitecture for hand-held devices](#) 2005

9. [Eisenbarth T;Güneysu T;Paar C Reconfigurable trusted computing in hardware](#) 2007

10. [Dietrich K An integrated architecture for trusted computing for java enabled embedded devices](#) 2007

11. [徐拾义 可信计算系统设计和分析](#) 2006

12. [冯登国;秦宇 可信计算环境证明方法研究](#) 2008(09)

13. [林闯;田立勤;王元卓 可信网络中用户行为可信的研究](#) 2008(12)

14. [王忠玉 基于生物进化选择的经济演化理论研究](#) 2006(03)

15. [刘海龙 对生物进化自组织理论具体机制的探讨](#) 2005(06)

16. [余有明;刘玉树 进化计算的理论与算法](#) 2005(09)

17. [李曙新 哈贝马斯的社会进化理论评析](#) 2004(04)

本文链接: http://d.wanfangdata.com.cn/Periodical_wjz201407025.aspx