Information Security Issues and Countermeasures in Academic Publishing: A Multi-Stakeholder Perspective

Authors: Duan Yaoqing, Zheng Zhuowen, Wang Rui, Zheng Zhuowen

Date: 2022-11-13T00:00:00+00:00

Abstract

Purpose: Analyzing the current status and existing problems of information security in scientific paper publication is conducive to enhancing our understanding of China' s holistic national security view and clarifying the future development direction of this field.

Methods: Based on full lifecycle theory, normative analysis and theoretical construction of information security issues in scientific paper publication are conducted from a multi-stakeholder perspective.

Results: An information security ecosystem for various contributing entities in scientific paper publication is constructed, and a five-dimensional integrated improvement path for information security in scientific paper publication from a multi-stakeholder perspective is proposed.

Conclusion: Information security issues in scientific paper publication represent one of the major theoretical and practical problems requiring correct understanding and grasp, constitute a brand-new subject under new external environments, new technological revolutions, and new competitive landscapes, and simultaneously call for new epistemology and methodology to deepen understanding of this issue.

Full Text

Information Security Issues and Countermeasures in Scientific Paper Publishing: A Multi-Stakeholder Perspective

Yaoqing Duan, Zhuowenyi Zheng, Rui Wang
Hubei Data Governance and Intelligent Decision-Making Research Center, School of Information Management, Central China Normal University

Nanhu Campus, Central China Normal University, 382 Xiongchu Avenue, Hongshan District, Wuhan, Hubei Province, 430079

Abstract

[**Purpose**] Analyzing the current state and existing problems of information security in scientific paper publishing enhances our understanding of China' s holistic national security concept and clarifies future development directions in this field. [**Method**] This study conducts normative analysis and theoretical construction of information security issues in scientific paper publishing from a multi-stakeholder perspective, grounded in whole lifecycle theory. [**Findings**] We construct an ecological system of information security for all contributing entities in scientific paper publishing and propose a five-dimensional integrated improvement path for information security from a multi-stakeholder viewpoint. [**Conclusion**] Information security in scientific paper publishing represents one of the major theoretical and practical issues requiring proper understanding and grasp. It is an entirely new topic emerging under novel external environments, technological revolutions, and competitive landscapes, necessitating new epistemological and methodological approaches to deepen comprehension of this issue.

Keywords: Scientific paper publishing; Information security; Problems and countermeasures; Improvement path

Corresponding Author: Zhuowenyi Zheng, 574144157@qq.com

Author Contribution Statement: Author 1: Proposed the ecological system of contributing entities in scientific paper publishing, the five-dimensional integrated improvement path for information security from a multi-stakeholder perspective, research direction, and paper framework; participated in paper revision. Author 2: Conducted literature review and compilation; wrote the paper. Author 3: Performed comparative experiments, data collection and analysis; revised the paper.

With the rapid development of artificial intelligence, big data, cloud computing, data mining, and blockchain technologies, digital transformation across various fields has entered a normalized stage, and China is gradually transitioning from an industrial society to an information society. This transition has generated massive volumes of business information circulating on the internet, which authentically reflects the operational conditions of the objective world and contains substantial social and economic value. If misused or stolen by malicious actors, such information could damage personal property and safety at minimum, and endanger social and national security at worst. In 2014, President Xi Jinping first proposed the twelve components of the holistic national security concept, identifying information security as a critical element. The report of the 19th National Congress similarly emphasized the importance of addressing both tra-

ditional and non-traditional security concerns, with information security falling into the latter category. To regulate internet information usage and safeguard information security, China has enacted multiple policies and regulations since 2015, including the National Security Law (2015), Cybersecurity Law (2017), Cryptography Law of the People' s Republic of China (2019), Data Security Law (2021), and Personal Information Protection Law (2021). Additionally, various industry standards such as the Regulations on Security Protection of Critical Information Infrastructure, Regulations on Network Data Security Management, and Information Security Technology - Personal Information Security Specification have been issued. The completion of this legal and regulatory framework marks the formation of a systematic structure for information security governance in China, gradually ushering the nation into a stage of legalized information security supervision.

However, the field of scientific paper publishing still faces numerous practical challenges, with frequent information security incidents occurring during the publication process. Throughout paper publication, substantial amounts of critical information regarding authors themselves, paper content, creative innovations, and research methodologies are leaked, severely damaging authors' intellectual property rights. Many published papers contain research findings and conclusions based on the collection and analysis of large volumes of factual data that reflect China' s actual development conditions. If such papers disregard national security considerations, they can cause serious adverse effects on national security and social stability. For research institutions and publishers, external information security threats are continuously escalating with rapid technological advancement. Factors such as business datafication, system digitization, and information networking have increased the risk of internal information leakage within research institutions. External forces exploit technical means like attacking information system vulnerabilities and circumventing protective measures to conduct theft, alteration, and illegal use of scientific paper information. Meanwhile, some internal management personnel can easily access critical information from unpublished papers through their privileges and positions, leading to information leakage, destruction, and loss. As the potential economic value of information becomes further recognized, activities seeking illegal information transactions on the dark web have become increasingly frequent. Data leaked by internal and external forces spreads more rapidly through dark web channels, enabling illegal actors to obtain higher returns, which further amplifies national security risks associated with scientific paper information security issues.

Current academic research on information security technology applications has yielded abundant results, primarily exploring the adaptability of technologies such as blockchain [1-2] and deep learning [3] to information security in environments like big data [4-5], cloud computing [6-7], and the Internet of Things [8-9], gradually constructing certain information security protection architectures. Scholars have also conducted in-depth discussions on network information security protection strategies [13-14], information security literacy [15], and influencing factors of network information security [16-18] across numerous fields

including finance [10], healthcare [11], and industry [12]. Although research in the specific domain of scientific paper publishing remains insufficient, the rich theoretical and practical achievements in the broader information security field provide a sufficient foundation for theoretical construction in scientific paper publishing information security.

2.1 Classification of Scientific Papers

Classification criteria for papers vary according to different standards. Scientific papers can be divided into six categories: by discipline type, they can be classified as social science academic papers and natural science academic papers; by discipline nature, they can be categorized as basic discipline academic papers and technical application discipline academic papers; by argumentation method, they include basic theoretical, methodological technical, survey report, literature review, applied research, and academic debate types; by writing content, they can be divided into thematic and comprehensive academic papers; by research scope, they can be classified as macro-research and micro-research academic papers [16]; and according to China' s national standard "Format for Scientific and Technical Reports, Dissertations and Scientific Papers," they can be categorized as journal articles and dissertations. Different types of scientific papers face distinct information security issues during publication. For instance, dissertations frequently suffer from academic misconduct, as novice researchers with insufficient theoretical knowledge often intentionally or unintentionally use others' core research findings, potentially infringing upon other authors' intellectual property rights if improperly handled. Additionally, dissertations are often printed at nearby commercial print shops and subjected to inexpensive third-party plagiarism checking services online, significantly increasing the risk of leakage. Journal article publication follows a different process, where authors submit manuscripts to journals and subsequent publication work is generally assisted by reviewers and editors. While the aforementioned information security issues may still occur, journal articles are more susceptible to unauthorized disclosure by privileged personnel before publication or illegal system intrusion by external forces during paper transmission and storage. Specific details are shown in Table 1 .

Table 1 Classification of Scientific Papers *By discipline type:* Social science academic papers, Natural science academic papers
By discipline nature: Basic discipline academic papers, Technical application discipline academic papers
By argumentation method: Basic theoretical type, Methodological technical type, Survey report type, Literature review type, Applied research type, Academic debate type
By writing content: Thematic academic papers, Comprehensive academic papers
By research scope: Macro-research academic papers, Micro-research academic papers

By national standard: Journal articles, Dissertations

2.2 Definition and Lifecycle of Scientific Paper Publishing

Based on definitions of data security, cybersecurity, and personal information security in the Data Security Law of the People' s Republic of China and the Cybersecurity Law of the People' s Republic of China, this paper defines information security in scientific paper publishing as: the adoption of necessary legal, technical, and managerial measures to prevent attacks, intrusions, interference, destruction, and illegal use of scientific paper publishing systems, as well as accidental incidents, ensuring that all types of information involved in each stage of paper publication remain in a state of lawful and compliant collection and utilization, and maintaining the capability to sustain such a secure state.

Scientific papers can generally be divided into seven structural components: research topic, research question, literature review, research design, research practice (investigation and empirical research), research findings, and research conclusions. Information security issues vary across these different sections. For example, the research topic section frequently faces academic plagiarism issues regarding creative innovations and research directions, while the research practice section may involve data sourced from other studies or risks of leaking state secrets.

The general process of scientific paper publishing roughly includes: topic selection, conceptualization, writing, submission, revision, plagiarism checking, and acceptance/rejection. If rejected, the paper begins a new lifecycle, as illustrated in Figure 1 [Figure 1: see original paper]. Each link in this lifecycle presents different information security risks. For instance, topics and concepts may plagiarize or steal others' ideas; writing may involve copying others' statements or unintentionally leaking state secrets; submission and revision often occur through online information systems, where multi-interface API transmissions face risks of hacker attacks and potential active disclosure by internal personnel. Therefore, it is necessary to clarify potential information security issues that may arise in each link during business practices of scientific paper publishing.

2.3 Constructing the Information Security Ecosystem of Contributing Entities in Scientific Paper Publishing

The successful publication of a scientific paper often results from the joint efforts of multiple entities. This paper constructs an information security ecosystem for contributing entities in scientific paper publishing, clarifying potential information security issues that may arise when three main contributing entities (authors, reviewers, and editors) interact with other entities during the publication process. Additionally, based on a multi-stakeholder perspective, we summarize the types of information security in scientific paper publishing as: personal information security, research group information security, institutional information security, disciplinary field information security, and national information

security.

As shown in Figure 2 [Figure 2: see original paper], the three main contributing entities—authors, editors, and reviewers—are both independent and closely interconnected, while individuals, research groups, institutions, disciplinary fields, and nations represent entities that may encounter information security issues during scientific paper publication. For example, scientific paper authors may intentionally or unintentionally affect the information security of other authors, research groups, research institutions, and disciplinary fields, with more severe cases potentially impacting national security. Similarly, reviewers and editors, as internal members of publishing institutions with access to scientific paper databases unavailable to general authors, may also affect the information security of other authors (individuals), research groups, institutions, disciplinary fields, and national security.

3 Problems in Information Security of Scientific Paper Publishing

The fundamental purpose of scientific paper publishing is to promote academic exchange and knowledge sharing, accumulate scientific achievements, and accelerate development across scientific fields. Therefore, the essence of scientific paper publishing is open sharing—research results should be publicly disclosed without discrimination to all researchers in need, facilitating academic exchange while contributing individual scholarly achievements to the broader research field to enable deeper exploration by subsequent researchers. However, information security emphasizes restricted access, confidentiality, and additional sharing conditions, which appears contradictory to the open nature of scientific paper publishing. Certain sensitive information in scientific papers requires protection and cannot be fully disclosed. Even when disclosed, such information must be recognized as the author' s intellectual property and cannot be arbitrarily used by others. For instance, research content, methodologies, data, and creative ideas from unpublished papers, once leaked before publication, severely damage authors' rights and gradually diminish their enthusiasm for originality. Additionally, some information involving current state secrets cannot be fully disclosed, such as information on national frontier technological development, latest military dynamics, or critical information on major emergencies. Unrestricted public disclosure of such information would become a tool for malicious actors and domestic or foreign hostile forces to endanger national security and social stability. This creates two major contradictions in scientific paper publishing information security: openness versus confidentiality, and knowledge sharing versus intellectual property rights. Resolving these contradictions—maximizing the deepening of scientific paper information sharing and circulation efficiency while ensuring confidential information security and protecting multi-stakeholder information security—represents an urgent challenge and a key future research direction.

Under these contradictory premises, current information security issues in China' s scientific paper publishing have generated several critical problems:

(1) Weak Personal Information Security Awareness Among Authors

Many scientific paper authors lack sufficient awareness of information security protection and frequently leak personal information or infringe upon others'information security, either intentionally or unintentionally. Numerous early-career researchers still print papers at commercial print shops and seek inexpensive, unregulated third-party plagiarism checking services online. These unconscious active disclosure behaviors by authors, combined with third-party institutions' motivations to obtain illegal profits, can easily result in scientific paper leakage before publication. Furthermore, some authors engage in plagiarism, misappropriation, and alteration of others' research findings in their personal papers, constituting academic misconduct and endangering other authors' scientific paper information security. Regarding state secrets, some authors lack political sensitivity and include confidential documents and information involving national security in their papers for public publication, which can be easily exploited by domestic and foreign hostile groups, elevating risks to national security.

(2) High Information Leakage Risks Among Privileged Personnel

Privileged personnel primarily refers to staff members of research institutions, reviewers, and editors who typically manage certain affairs in scientific paper publishing and can access sensitive information through their positions. For example, some management personnel within national research institutions can grasp the latest developments in China' s classified scientific and technological advancements and use this information for paper creation, endangering national security. In 1999, a case occurred in China where classified parameter information of the J-10 fighter jet was leaked in a paper, with the leaker being an assistant engineer at a Chinese research institute. Additionally, some editors and reviewers at journals and research institutions can access unpublished papers and unapproved project proposals, enabling them to plagiarize, alter, and sell such materials, causing severe damage to contributors' intellectual property rights. Overall, privileged personnel can easily access critical information, yet institutional management of them remains relatively lax, resulting in frequent information security incidents.

(3) Technological Advancements Increasing Security Supervision Difficulties

Currently, computer and big data analysis technologies are increasingly mature, and institutional operations have undergone digital transformation. Almost all business in scientific paper publishing can now be completed through the internet and information systems, providing researchers with more convenient ways to obtain and utilize data while greatly improving publication efficiency. However, the continuous maturation of internet technology also means researchers can more easily access others' research findings and other valuable paper information online, directly appropriating others' topics, concepts, methods, creative ideas, and data. Some authors also use advanced web scraping technologies to conduct deep data crawling of social media platforms, organizational websites,

and classified databases on government websites when collecting data related to national economy and people' s livelihood, employing illegal and non-compliant means to obtain privacy information concerning individuals and national security. Although major internet platforms continuously update anti-scraping technologies, some malicious actors still manage to bypass protective measures and successfully scrape relevant classified information. The anonymity of internet interactions helps malicious actors better conceal their identities, while powerful data analysis tools (web scraping technology, data mining technology, data desensitization technology, etc.) enable them to conduct illegal theft activities at lower costs.

From the perspective of research management information system usage, current business systems are typically accessed through multiple devices including mobile phones, desktop computers, laptops, and tablet computers. While this multi-device interconnected business operating system provides convenience for scientific paper publishing, the differing system architectures and technologies of various devices expose them to more diverse forms of external hacker attacks. Moreover, besides storing scientific papers on local physical hard drives, more authors now choose to store papers and data on cloud drives, further exacerbating information leakage risks. Additionally, scientific paper publishing systems typically have multiple API interfaces, such as email and plagiarism checking service interfaces, which become important pathways for external hackers to attack systems and obtain scientific paper data during transmission. Overall, technological advancements continuously introduce new methods of endangering information security while bringing convenience to scientific paper publishing.

(4) Absence of Industry Policy Standards

While numerous laws and regulations have been issued in the data security field, such as the Cybersecurity Law, Personal Information Protection Law, Data Security Law, and Regulations on Network Data Security Management (Draft for Comment), the scientific paper publishing field still lacks systematic, specialized, and unified policy standards. Compared with the comprehensive information security protection legal systems and industry guidance standards already established in finance and industry sectors, only a few policy documents specifically targeting scientific paper publishing have been issued nationally, such as the Management Measures for Classified Graduate Students and Classified Dissertations (2016) and the Management Measures for Scientific Data (2018). The attention given to policy standards in this field remains far from sufficient compared to the well-developed policy and regulatory systems in finance and industry.

4 Countermeasures and Recommendations for Information Security in Scientific Paper Publishing

Addressing the aforementioned critical problems, this paper proposes a five-dimensional integrated improvement path for information security in scientific

paper publishing from a multi-stakeholder perspective, as illustrated in Figure 3 [Figure 3: see original paper]. In this framework, cognition serves as the premise, law provides the guarantee, technology and management serve as the means, and business constitutes the primary practice arena.

(1) Cognitive Dimension

Authors, research groups, and institutions must first recognize the importance of information security protection in scientific paper publishing and comprehensively learn and deeply understand the manifestations of information security, behaviors that may cause information security problems, and primary avoidance methods. Continuous training on information security issues in scientific paper publishing should be conducted through lectures, forums, and specialized courses to enhance authors' information security literacy. Disciplinary fields and the nation need to attach importance to the development and research in this domain, clarifying the main contradictions, relevant stakeholder interests, and future development directions of information security in scientific paper publishing. Only by understanding the connotations and importance of these issues can better policies and standards be formulated, relevant technical and management measures introduced, academic research in this area guided, and business practices directed.

(2) Legal Dimension

Laws, regulations, and policy standards should be utilized to guide and guarantee the orderly development of information security governance activities in scientific paper publishing. Based on existing national data security laws, regulations, and industry standards, and referencing information security laws, regulations, and standards from more mature and leading industries such as finance and industry, a comprehensive legal guarantee system should be constructed for scientific paper publishing, covering information security standards, information security level assessment, and management measures. This would perfect the top-level legal architecture design, ensuring that individuals, research groups, institutions, and industries have laws to abide by and standards to implement.

(3) Technological Dimension

The nation, industries, and institutions should actively introduce new information technologies to develop unified paper publishing platforms that maximize collaborative sharing of paper information while improving machine automatic processing efficiency, reducing manual intervention by authors, reviewers, and editors, and lowering leakage risks. Federated learning should be employed to solve information collaboration and fusion problems during scientific paper publishing under non-open scenarios, accelerating information circulation across platforms and achieving cross-platform, cross-business, and cross-level information fusion while ensuring information security. This approach both protects intellectual property rights and promotes knowledge exchange efficiency, properly resolving contradictions between "openness and confidentiality" and "knowledge sharing and intellectual property rights." Additionally, core concepts from

blockchain encryption technology such as identity chains, data proof, and smart contracts can be adapted to establish protection models for information ownership, usage rights, and revenue rights in scientific paper publishing across different stages (creation, fusion, exchange) and different entities (authors, reviewers, editors, platforms). To prevent on-chain information from being abused by users, an information-proof-based usage authorization mechanism can be established to ensure information can only be accessed with creators' and managers' permission. Furthermore, artificial intelligence and natural language recognition technologies can be introduced to improve machine accuracy in automatically recognizing scientific paper text, enabling more effective plagiarism detection not only for conventional phrases and sentences but also for critical yet difficult-to-identify components such as creative ideas, data sources, and research methodologies. This would more sensitively and accurately detect content where authors use data desensitization and other technologies to evade machine plagiarism detection.

(4) Management Dimension

Current scientific research work is characterized by high informatization, significant leakage risks, rapid technological updates, more flexible research venues, numerous participants, complex personnel composition, and high frequency of new researchers. Targeted management measures such as regular training, publicity, accountability, and review should be implemented to strengthen researchers' information security awareness and capabilities. Research institutions should formulate appropriate ethical norms and management measures for scientific paper publishing, appoint dedicated personnel to supervise reviewers, editors, and submission systems, clarify authority and responsibility boundaries, and establish mutual supervision and restraint mechanisms to prevent privileged personnel within institutions from illegally accessing scientific paper information through their positions. Simultaneously, regular security screenings of scientific paper publishing information systems should be conducted to promptly identify and respond to external attacks, with regular virus scans performed on key personnel' s computers, accounts, emails, and hard drives to reduce external attack risks.

(5) Business Dimension

Business practice in scientific paper publishing represents the outcome of comprehensive application of cognitive premises, legal guarantees, and technological and management measures, while simultaneously influencing the other four dimensions. Disciplinary fields and research institutions need to recognize the impacts of the other four dimensions on business practice, improve top-level design by providing legalized, procedural, and standardized policy systems as guarantees, and construct unified scientific paper publishing management platforms using technologies such as blockchain, federated learning, and artificial intelligence as carriers. Regular review and accountability activities should be implemented as management measures to constrain excessive use of privileges by relevant privileged entities and protect contributors' intellectual property rights.

Concurrently, business practice requires collecting substantial feedback from authors, research groups, research institutions, and disciplinary fields, which can reflect actual needs of different entities in business practice and evaluate the operational effectiveness of currently implemented policies, technologies, and management measures, facilitating improvement and optimization in subsequent stages. The five-dimensional integrated improvement path system forms a virtuous development cycle, with the five dimensions mutually influencing and complementing each other to steadily enhance information security in scientific paper publishing.

Figure 3 Five-Dimensional Integrated Improvement Path for Information Security in Scientific Paper Publishing

This paper discusses the classification, structure, publication lifecycle, and definitions of scientific papers, constructs an information security ecosystem for contributing entities in scientific paper publishing from a multi-stakeholder perspective, and summarizes different types of information security issues faced by different entities. We argue that information security in scientific paper publishing involves three key understandings: First, it represents one of the major theoretical and practical issues in information security that requires proper understanding and grasp. Second, it is an entirely new topic, specifically manifested in new problems brought by new external environments, new technological revolutions, and new competitive landscapes. Third, it calls for new epistemological and methodological approaches to deepen interpretation of this issue, such as value orientation, bottom-line thinking, and balanced thinking in paper publishing.

References

[1] Liu Aodi, Du Xuehui, Wang Na, Li Shaozhuo. Blockchain technology and its research progress in the field of information security[J]. Journal of Software, 2018,29(07):2092-2115.
[2] Wu Zhenquan, Liang Yuhui, Kang Jiawen, Yu Rong, He Zhaoshui. Smart grid data security storage and sharing system based on consortium blockchain[J]. Computer Applications, 2017,37(10):2742-2747.
[3] Sun Hao, Chen Jin, Lei Lin, Ji Kefeng, Kuang Gangyao. A survey on adversarial robustness techniques of deep convolutional neural network image recognition models[J]. Journal of Radars, 2021,10(04):571-594.
[4] Wang Shiwei. On the new characteristics and requirements of information security in the era of big data[J]. Library and Information Service, 2016,60(06):5-14.
[5] Zhang Maoyue. Risks and responses for citizens' personal information data in the era of big data[J]. Information Studies: Theory & Application, 2015,38(06):57-61+70.
[6] Xue Yan, Zhu Xuefang. Research on cloud computing user privacy protection based on improved encryption algorithm[J]. Information Science, 2016,34(09):145-149.

[7] Qiu Rongrong, Hu Changping. Research on collaborative governance framework for national digital academic resource information security in cloud computing environment—Based on information ecology perspective[J]. Library and Information Service, 2022,66(08):55-62.
[8] Wu Wufei, Li Renfa, Zeng Gang, Xie Yong, Xie Guoqi. A survey on cybersecurity of intelligent connected vehicles[J]. Journal on Communications, 2020,41(06):161-174.
[9] Song Tao, Li Xiuhua, Li Hui, Wen Junhao, Xiong Qingyu, Chen Jie. A survey on security encryption and authentication technology for internet of vehicles in the era of big data[J]. Computer Science, 2022,49(04):340-353.
[10] Jin Yuhong. Research on information security prevention and guarantee system for internet finance in big data environment[J]. Information Science, 2018,36(12):134-138.
[11] Li Hongchen, Ma Jie, Hu Mo. Construction of medical blockchain model for health big data security protection[J]. Library and Information Service, 2021,65(02):37-44.
[12] Jin Jianghong, Mo Changyu, Li Gang. Research on integrated protection measures for functional safety and information security of industrial control systems[J]. Industrial Safety and Environmental Protection, 2020,46(01):53-60.
[13] Leng Xiaoyan. Research on information security strategy in the era of big data[J]. Information Science, 2019,37(12):105-109.
[14] Zhang Yanfeng, Wang Yuxi, Zou Kai, Peng Lihui. Research on risk factor identification and management strategy of smart city information security based on fuzzy DANP[J]. Information Studies: Theory & Application, 2020,43(10):144-150.
[15] Chen Qi, Xiong Huixiang, Dai Xinquan, Gu Jiayun. Research on evaluation and improvement strategy of college students' network information security literacy capability from the perspective of platform society[J]. Library and Information Service, 2022,66(07):75-87.
[16] Wang Xiwei, Wang Lei, Jia Ruonan, Wang Duo. Empirical study on influencing factors of personal information security behavior in social networks[J]. Library and Information Service, 2018,62(18):24-33.
[17] Zou Kai, Xiang Shang, Zhang Zhongqingyang, Mao Taitian. Construction and empirical study of smart city information security risk assessment model[J]. Library and Information Service, 2016,60(07):19-24.
[18] Zhou Fengfei, Wang Jiajia. Investigation and analysis of information security awareness and behavior of smartphone users among college students[J]. Library and Information Service, 2018,62(10):47-53.
[19] Yao Xianguo et al. Guidance for Economics Students on Thesis Writing[M]. Hangzhou: Zhejiang University Press, 2004: 4.

Note: Figure translations are in progress. See original paper for figures.