Scholars Journal of Engineering and Technology
OPEN ACCESS
Abbreviated Key Title: Sch J Eng Tech
ISSN 2347-9523 (Print) | ISSN 2321-435X (Online)
Journal homepage: https://saspublishers.com

Forging Ethical Guardians of Cyberspace: A Cryptography-Infused Model for Scalable Engineering Ethics Education

Yuanyuan Huang[1*], Shuo Han[2], Cong Wang[1], Yunyi Huang[1], Peilin He[3]

[1]School of Artificial Intelligence, Chengdu University of Information Technology, Chengdu, 610225, China
[2]Department of Computer Science, University College London, London, WC1E 6BT, UK
[3]Department of Informatics and Networked Systems, University of Pittsburgh, Pittsburgh, PA 15260, USA

DOI: https://doi.org/10.36347/sjet.2026.v14i03.001 | **Received:** 17.01.2026 | **Accepted:** 25.02.2026 | **Published:** 03.03.2026

***Corresponding author:** Yuanyuan Huang
School of Artificial Intelligence, Chengdu University of Information Technology, Chengdu, 610225, China

Abstract | **Review Article**

As cyberspace security becomes a global imperative, the cultivation of ethically responsible professionals in foundational disciplines such as cryptography is increasingly critical. However, current engineering ethics curricula often fail to address the distinctive and profound dilemmas inherent in cryptology, and this gap persists across both undergraduate and postgraduate education. To address this gap, this paper proposes a novel and scalable pedagogical framework "Value-Nurturing, Knowledge-Integration, and Competency-Immersion" designed for implementation across the higher education continuum. We conceptualize a tiered approach where ethical competence evolves from foundational awareness at the undergraduate level to strategic reasoning at the postgraduate level. The framework integrates technical rigor with ethical reflection through three dimensions: (1) anchoring values within the sociotechnical narrative of cryptology; (2) embedding ethical discourse into core technical courses through a scaffolded curriculum design; and (3) employing progressively scenario-based training. Drawing on implemented practices from multiple institutional contexts, we demonstrate how this framework fosters the cultivation of "Ethical Guardians" capable of navigating dilemmas ranging from algorithm design to policy implications.

Keywords: Engineering Ethics Education; Cryptography; Cyberspace Security; Curriculum Reform; Value Cultivation; Scaffolded Pedagogy.

1 INTRODUCTION

The security of modern digital infrastructure is fundamentally underpinned by cryptography [1]. Accordingly, graduates in cyberspace security and cryptology from the bachelor's to the doctoral level are entrusted with the tools that safeguard privacy, integrity, and trust on a global scale. Their work extends beyond mathematical formalism or software implementation; it involves value-laden decisions situated at the intersection of technology, law, and human rights [7]. Whether an undergraduate selecting an encryption mode for a course project or a postgraduate researcher contributing to a national cryptographic standard, ethical reasoning must be cultivated as a core competency.

Despite the centrality of ethical reasoning in cryptology, a significant pedagogical gap persists across educational tiers. Ethics instruction is frequently confined to a single, generic course, leaving students ill-equipped to translate broad principles into the specific, often abstract, ethical quandaries of their discipline. These dilemmas include tensions between privacy and lawful access, the global nature of algorithms versus national sovereignty, and the societal consequences of implementing (or weakening) cryptographic protocols [1,7].

This paper addresses the dual challenge of disciplinary specificity and educational scalability. We propose a comprehensive pedagogical framework that integrates cryptography-specific ethics throughout a multi-year curriculum, tailored to the cognitive and professional development stages of both undergraduate and postgraduate students. Our approach repositions ethics from a peripheral "add-on" to a central and integrative thread in the formation of cyberspace security professionals. The paper concludes with a discussion on adaptable implementation strategies across diverse academic programs.

2. A Tiered Educational Framework: From Awareness to Strategic Judgment

Building on established frameworks for engineering ethics education [3, 4], we propose a model that rests on three interconnected pillars---Value-Nurturing, Knowledge-Integration, and Competency-Immersion---implemented with progressively greater depth across undergraduate (UG) and postgraduate (PG) levels.

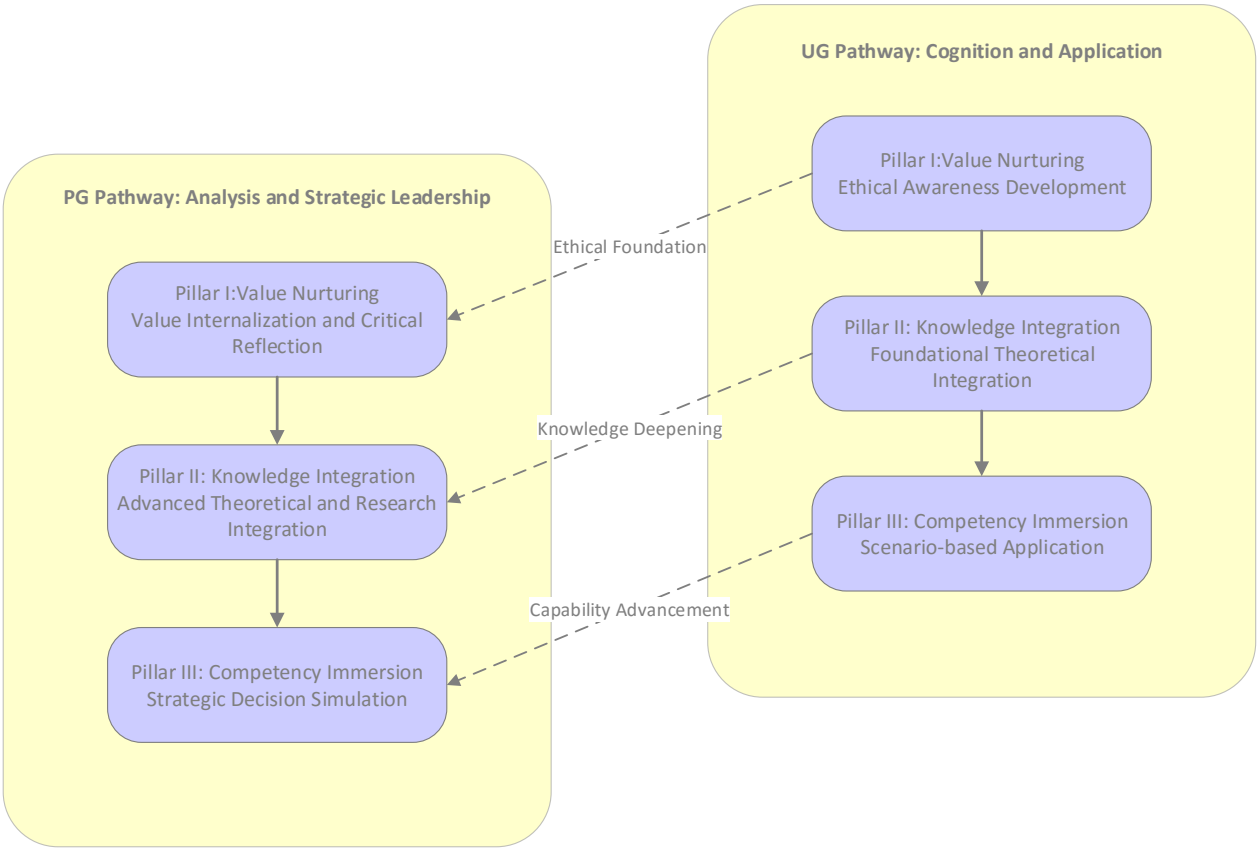

Figure 1: Tiered Cryptography Ethics Education Framework

2.1. Pillar I: Value-Nurturing – Cultivating a Professional Ethos

The goal is to cultivate an identity of responsible custodianship, evolving from basic recognition to internalized commitment.

Undergraduate Focus (Awareness & Role-Modeling): Introduce the societal role of cryptography through historical narratives (e.g., the Enigma story, the public-key revolution) and contemporary controversies (e.g., the Apple-FBI case) [1]. Emphasize professional codes of ethics from bodies such as the ACM/IEEE, highlighting principles of honesty, confidentiality, and public good.

Postgraduate Focus (Internalization & Critical Reflection): Engage in deep critical analysis of the sociopolitical dimensions of cryptography. Explore ethical considerations of "algorithmic sovereignty" (e.g., national cryptographic standards), the philosopher's role of the cryptographer in society, and the tension between academic openness and potential dual-use risks. Reflect on individual responsibility within complex systems.

2.2. Pillar II: Knowledge-Integration – Weaving Ethics into the Technical Core

Ethics is integrated as an applied lens throught the technical curriculum, with complexity increasing across levels.

Undergraduate Tier:

Foundational Courses: In an Introduction to Cryptography, discuss why textbook RSA is insecure in practice, linking to the ethical responsibility of implementing proven, standards-based cryptography. In a Network Security course, frame the use of VPNs and HTTPS within debates on privacy versus lawful interception.

Project Work: Require a brief "ethical impact paragraph" in project reports, prompting students to identify potential misuse or societal consequences of their designed systems.

Postgraduate Tier:

Advanced Courses: In a Secure Protocol Design course, mandate an "Ethical Design Appendix" evaluating protocol choices against fairness (e.g., non-discriminatory access), transparency, and potential for

coercion. In a Blockchain seminar, analyze the environmental ethics of consensus mechanisms.

Research Seminars: Dedicate sessions in Post-Quantum Cryptography or Multi-Party Computation to "risk forecasting," where students research and present the ethical and societal disruption arising from technological transitions.

2.3. Pillar III: Competency-Immersion – Progressive Ethical Decision-Making

Students practice applying values and knowledge in progressively complex and ambiguous scenarios.

Undergraduate Methods: Utilize focused case studies and structured role-plays. For example, a case study on the 2013 "Dual_EC_DRBG" backdoor suspicion can illustrate standards-setting ethics. A role-play might involve a developer facing pressure to cut corners on cryptographic implementation to accelerate the product release.

Postgraduate Methods: Employ high-fidelity simulations and strategic dilemma exercises. A simulation could involve a multi-stakeholder "National Digital Policy Working Group" debating legislation on encryption. A dilemma exercise might task students with developing an ethical disclosure policy for a research lab that uncovers a critical vulnerability in widely used financial infrastructure.

3 Implementation Strategies and Adaptable Case Examples

The successful implementation of this framework requires integration at the program level rather than as isolated courses.

3.1 Curriculum Mapping and Scaffolding:

A program should map where and how each pillar is addressed across its core courses.

Year 1-2 (UG): Introduce core ethical principles and historical context in introductory courses. Incorporate guest lectures from alumni in law or policy.

Year 3-4 (UG/PG Taught Masters): Embed ethics modules within advanced technical courses (e.g., system security, applied cryptography). Implement substantial ethics-based assignments within capstone projects.

Year 5+ (PG Research): Integrate ethics into research lab culture through mandatory reading groups on responsible innovation and ethics reviews of research proposals.

3.2 Adaptable Case Example: The "Secure Messaging App" Design Sprint

This multi-level activity can be adapted for a sophomore project or a postgraduate workshop.

Scenario: A student team assumes the role of the engineering division of a startup developing a new secure messaging app for a global market.

Tiered Tasks:

Undergraduate Version: Focus on implementation decisions. Students must select cryptographic protocols (e.g., Signal Protocol), justify their choices based on security and ethical considerations (e.g., open-source for auditability), and draft a privacy policy for end-users in accessible language.

Postgraduate Version: Focus on strategic dilemmas. Students must develop a company-wide policy for responding to lawful access requests from different jurisdictions, design a technical architecture aligned with this policy, and prepare a briefing for the board outlining the potential business and human rights trade-offs.

Learning Outcome: UG students understand the direct link between implementation choices and user trust. PG students engage with the complex interplay of technology, law, business, and ethics at a systemic level.

3.3 Institutional Practices from the Field:

Module Integration: Drawing on models in Chinese engineering education research [5,6], several programs have successfully embedded "ethical impact analysis" as a required component of final-year project documentation and thesis proposals.

Interdisciplinary Collaboration: Effective programs often co-teach advanced ethics modules with faculty from law, philosophy, or public policy departments, exposing students to diverse analytical frameworks [7].

Assessment Innovation: Moving beyond essays, assessment includes peer evaluation in role-plays, analysis of ethics statements in real-world cryptographic standards (e.g., NIST FIPS publications), and reflective portfolios tracing the evolution of a student's ethical reasoning over time.

4. Discussion: Addressing Challenges and Ensuring Scalability

Implementing this model presents common challenges across institutional contexts.

Faculty Preparedness: Technical faculty may lack training in facilitating ethics. Solution: Develop a supportive "teaching kit" with discipline-specific case studies, discussion guides, and develop communities of practice via regular workshops [8,9].

Curriculum Crowding: Adding content can face resistance. Solution: Emphasize integration rather than addition. Show how ethical discussion reinforces deep technical understanding (e.g., debates over backdoors demand an understanding of key management).

Avoiding Prescriptivism: The goal is ethical reasoning, not indoctrination. Pedagogy must prioritize open debate, exploration of gray areas, and exposure to multiple legitimate perspectives within professional boundaries.

Scalability for Different Programs: The framework's tiered nature allows flexibility. Teaching-focused undergraduate institutions can emphasize Pillars I and II with strong competency exercises, while research-intensive universities can implement advanced Pillar III simulations for postgraduate students, building on the undergraduate program as a foundational pipeline. These design considerations are informed by ongoing discourse in the field [8].

5. CONCLUSION

The era of treating cryptography as a purely technical domain is over. Educating the next generation of cyberspace guardians requires a deliberate, scaffolded approach to ethical development that both parallels and informs their technical growth. The "Value-Nurturing, Knowledge-Integration, and Competency-Immersion" framework offers a flexible model for this crucial integration.

By starting with ethical awareness at the undergraduate level and progressing to strategic judgment at the postgraduate level, academic institutions can systematically cultivate professionals who are not only cryptographically competent but also ethically resilient. These individuals will be equipped to make sound decisions whether implementing a line of code, contributing to an open-source library, advising on a national standard, or testifying before a parliamentary committee. The security of our future digital society depends on this holistic foundation of trust and responsibility. Future work should focus on developing shared repositories of open-source teaching materials and conducting longitudinal studies to access the career-long impact of such integrated ethics education.

Acknowledgement

This work is supported by the Postgraduate Teaching Research and Reform Project of Chengdu University of Information Technology (No. CUITGOKP202419, No. PDCL202407) and the Undergraduate Teaching Research and Reform Project of Chengdu University of Information Technology (No. JYJG2024182, No. JYJG2025035).

REFERENCES

1. Abelson, H., Anderson, R., Bellovin, S. M., *et al.,*(2015). Keys under doormats: mandating insecurity by requiring government access to all data and communications. *Journal of Cybersecurity*, 1(1), 69-79.
2. Tavani, H. T. (2016). *Ethics and technology: Controversies, questions, and strategies for ethical computing* (5th ed.). Wiley.
3. Davis, M. (2006). Integrating ethics into technical courses: Micro-insertion. *Science and Engineering Ethics*, 12(4), 717-730.
4. Herkert, J. R. (2005). Ways of thinking about and teaching ethical problem solving: Microethics and macroethics in engineering. *Science and Engineering Ethics*, 11(3), 373-385.
5. Ao, T. (2023). Exploration and Practice of Ideological and Political Education in Engineering Talent Training: A Case Study of Network Engineering Curriculum. *Software Guide*, 22(6), 263-267.
6. Lu, B., Li, G., Huang, H., *et al.,*(2024). Construction of an Online Teaching System for 'Engineering Ethics' Integrating OBE Concept and Curriculum Ideology. *Journal of Nanchang Hangkong University (Natural Science Edition)*, 38(3), 121-126.
7. Zhu, J., & Shi, J. (2025). New Exploration of Collaborative Education between Ideological and Political Courses and Curriculum Ideology. *News from the School of Marxism, Changzhou University*.
8. Si, X., & Pan, H. (2025). Central Plains Forum Summary of the Forum on Cyberspace Security Discipline Construction and Postgraduate Academic Innovation. *News from Zhongyuan University of Technology*.
9. Wang, D. (2025). Engineering Ethics and Decision-Making Trade-offs: Challenges and Responses in Practice. In *Case Study Showcase of Curriculum Ideology*.