

Article Review #2 The Philosophy of Cryptography

Relations to The Principles of The Social Sciences

Cryptography, as addressed in the essay "Adversary: The Philosophy of Cryptography," has an inherent connection to social science principles, notably those concerning trust, power dynamics, and security. The study of cryptography systems reveals how societies organize to protect information, establish secure connections, and maintain privacy. These elements are relevant to social science fields including sociology, political science, and economics, which study the interaction of security mechanisms and societal structures. Cryptographic protocols, for example, are frequently designed to manage risks provided by competitors, which is like social theories of rivalry, collaboration, and democracy (Halpin, 2025).

Research Question and Hypotheses

The study's research questions or hypotheses focus mainly on the philosophical and ethical implications of cryptography. The project aims to answer fundamental concerns like, "How does cryptography influence power dynamics in digital societies?" What ethical concerns arise from the usage of encryption and security measures? Another hypothesis being investigated is whether cryptographic systems can enable equal access to security, particularly for

marginalized groups. The paper also examines the influence of adversaries in driving the evolution of cryptographic techniques (Halpin, 2025).

Research Methods and Analysis

The study's research methodologies are mostly qualitative and theoretical, including philosophical analysis, historical case studies, and comparative research. The article contextualizes cryptography's evolution within larger societal trends by evaluating historical examples of its application, such as wartime encryption and contemporary cybersecurity measures. It also conducts conceptual analysis, assessing various theoretical frameworks that support cryptographic techniques, such as adversarial thinking and trust models. In addition, policy analysis is used to evaluate how various governments and organizations manage and execute cryptographic technologies (Halpin, 2025).

Challenges, Concerns and Contributions

One of the study's strengths is its assessment of marginalized groups' challenges, concerns, and contributions. Cryptography is critical in ensuring safe communication for sensitive populations such as journalists, activists, and political dissidents. The study demonstrates how restrictive cryptographic practices, such as government-imposed encryption backdoors disproportionately affect underprivileged communities subjecting them to monitoring and persecution. Furthermore, it analyzes the digital divide and the potential difficulties that disadvantaged groups have in gaining access to powerful encryption technologies.

Overall Contributions to Society

Overall, the study benefits society by providing a better understanding of cryptography's role in shaping digital interactions, government, and personal freedom. It explores how encryption technology might be utilized to improve security while simultaneously generating ethical questions about privacy and power disparities. By investigating the adversarial character of cryptographic systems, the study contributes to policy discussions on cybersecurity, digital rights, and the ethical responsibilities of cryptographic designers. Finally, the study emphasizes the necessity of ensuring that cryptographic developments benefit not only governments and corporations, but also individuals and marginalized populations.

Relevance to PowerPoints

This paper uses archival research, which allows them to find historical cases and use comparative research to help them with their research methods and analysis. Although archival research is easily accessible, they may run into missing data and ethical issues, if they use information from the internet that was not meant to be used.

Conclusion

To summarize, cryptography is more than just a technical subject, it is an important social construct that affects and is influenced by power, trust, and fairness. The study of cryptography via a philosophical and social science perspective demonstrates its enormous impact on society,

notably in terms of individual rights and digital governance. As the digital ecosystem evolves, recognizing and fighting for inclusive and ethical cryptography policy will remain critical to promoting a more secure and equal world.

References

Harry Halpin. (2025) *The adversary: the philosophy of cryptography*

<https://academic.oup.com/cybersecurity/article/11/1/tyaf006/8097877?searchresult=1>