Cryptography at the Crossroads: Ethical Responsibility, the Cypherpunk Movement and Institutions

Eric Blair

Anonymous
eric.blair1912@proton.me

Abstract. This paper explores the intersection of cryptographic work with ethical responsibility and political activism, inspired by the Cypherpunk Manifesto and Phillip Rogaway's analysis of the moral character of cryptography. The discussion encompasses the historical context of cryptographic development, the philosophical underpinnings of the cypherpunk ideology, and contemporary challenges posed by mass surveillance and privacy concerns. By examining these facets, the paper calls for a renewed commitment to developing cryptographic solutions that prioritize human rights and societal good.

1 Introduction

Cryptography has long been a tool for securing communications and protecting privacy. However, its role extends beyond technical implementations to encompass significant political and ethical dimensions. The Cypherpunk Manifesto [7], penned by Eric Hughes in 1993, highlights the inherently political nature of cryptography and advocates for its use as a means of ensuring privacy and individual freedoms. Similarly, Phillip Rogaway's [10] work underscores the ethical responsibilities of cryptographers, particularly in the context of mass surveillance and societal impacts.

Fundamentally, cryptography can be seen as a means of "arming" the masses to protect themselves. The 1993 manifesto and Rogaway's work emphasize two key points: distrust of government and the protection of collective data. This perspective is echoed in the ideas of David Chaum, who proposed a transaction model relying on strong encryption to preserve privacy. Despite over 40 years passing since these ideas were first articulated, the dream of protecting society from the misuse of information remains distant. As Chaum warned:

> "[C]omputerization is robbing individuals of the ability to monitor and control the ways information about them is used. (...) The foundation is being laid for a dossier society, in which computers could be used to infer individuals' lifestyles, habits, whereabouts, and associations from data collected in ordinary consumer transactions" [5].

In reality, we have moved in a different direction. Today, we rely on such data to simplify and enhance our lives. Moreover, we willingly provide this data to make devices "smarter" and more tailored to our needs. On one hand, this gives us more time to focus on other tasks, such as developing advanced AI techniques. On the other hand, we have forgotten the essence of why cryptography is necessary and what the original dream was.

---

* Date of this document: 2024-06-16.
sha1sum: c7220050d72e8e6d4bcc9de832a11bc3f2186b59
This document continue to be updated as we get more understand and views about the subject.

The shift from a privacy-centric view to one that embraces data sharing for convenience highlights a significant ethical dilemma. While technological advancements have made life easier, they have also increased the risk of creating a surveillance society. The cypherpunk ethos, which aimed to empower individuals and protect their privacy, seems at odds with contemporary practices. To reconcile these differences, it is crucial for cryptographers and privacy advocates to reignite the original vision of cryptography—not just as a tool for convenience, but as a means to uphold privacy, autonomy, and resistance to unchecked surveillance.

Another shift in paradigms involves the connection between cryptography and anarchism. As articulated in the original crypto-anarchist manifesto, the ideas of anarchism and the use of cryptography were tightly intertwined. In essence, cryptography was seen as a tool for advancing anarchist principles. Anarchism, with its stance against all forms of authority and its call for the abolition of institutions, found a natural ally in cryptographic techniques.

In some ways, modern cryptographic practices continue to challenge institutional authority. However, there is a paradox: while cryptography aims to resist centralized control, its development and implementation are often dictated by experts and funded by major tech corporations and institutions. This creates a tension between the anarchist ideals of decentralization and the reality of cryptographic innovation being driven by powerful entities. To truly honor the cypherpunk and anarchist visions, it is essential to find ways to develop and deploy cryptographic tools that empower individuals while resisting the consolidation of power in any form.

There is also an ironic paradox in our community concerning the centralization of knowledge. One of the policies and mottos of the beloved IACR was to spread knowledge worldwide. The original and pure idea was great; however, somewhere along the path, this idea got corrupted. Consider the purpose of a non-profit organization. The term "**non-profit**" is clear. Yet, at every IACR meeting, one of the first slides presented is, "we have a robust financial position." Funnyly enough, for an association that wants transparency, it is very hard to find data about the "financial" besides attentind to the meetings. Furthermore, each year, we see the conference fees and the amount of money in our funds increase, while the original goal of sharing knowledge seems more distant, or just a utopia.

To cut to the chase, we have used the early days of anarchism, professors, and the fun times of building cryptography to simply construct a masked corporation under the guise of academic endeavors. This shift away from the foundational principles of both cypherpunk and anarchist visions demonstrates a need to return to the roots of cryptographic development—ensuring that it remains a tool for empowering individuals and safeguarding privacy against all forms of centralization and control.

In this work, we aim to present a comprehensive social view of cryptography and the entities that have made cryptographic advancements possible over the years. We will explore the ethical responsibilities, the origins of social movements that cryptography has influenced, and the current trajectory of cryptographic development. A key focus will be tracing the historical importance of cryptography and how it has shaped various aspects of our society. By examining these elements, we hope to provide a deeper understanding of the multifaceted role of cryptography in the modern world.

2 Historical context of Cryptography and its Implications

Originally, cryptography was defined as a branch of mathematics and computer science focused on developing techniques to encrypt and decrypt communications. Today, however, the scope of cryp-

tography has expanded significantly. While it still has its roots in mathematics, modern cryptography encompasses computer science, electrical engineering, physics, and several other disciplines. Therefore, a more comprehensive definition of *modern cryptography* is: "Cryptography is a multidisciplinary field dedicated to the study of digital security, aiming to provide tools that ensure the security of communications."

The development of cryptography has been profoundly influenced by its use in wartime communications and its evolution into digital security applications. Some key historical milestones include:

- **World War II and the Enigma Machine**: The use of cryptography for military communication and its decryption by the Allies highlighted the dual nature of cryptographic work as both a tool for security and a target for adversaries.
- **The Advent of Public Key Cryptography**: The introduction of public key cryptosystems in the 1970s revolutionized secure communications, laying the groundwork for modern cryptographic practices.
- **Shor's Algorithm and Factoring Primes**: The development of a quantum algorithm capable of breaking modern public key cryptography deployed worldwide.

Cryptography made significant advancements during World War II, a period marked by intense cryptographic and cryptanalytic activities. The successes in cryptanalysis during this time underscored the importance of rigorous analysis and the potential vulnerabilities in encryption methods.

As the computer industry expanded and the demand for secure hardware and software in the private sector grew, restrictive administrative regulations on the domestic use and export of encryption—initially classified as a war munition—became outdated. Ongoing technological advancements required state-of-the-art security measures [6]. This combination of distrust in data collection and outdated regulations led to the advocacy for encrypted technologies, which became both a market necessity and a form of resistance against increasing surveillance ecosystems.

A significant scientific breakthrough in cryptography came with the development of Shor's algorithm in the mid-1990s. This quantum algorithm efficiently solves problems such as integer factorization and discrete logarithms, which form the basis of many classical cryptographic systems like RSA and ECC. The advent of Shor's algorithm has spurred the development of post-quantum cryptography, which aims to create cryptographic algorithms that are secure against quantum attacks. This has become a crucial area of research, as the potential future realization of quantum computers threatens to undermine the security of current cryptographic systems. Ensuring the transition to quantum-resistant cryptographic methods is vital for maintaining the integrity and security of digital communications in the post-quantum era.

Standardization bodies such as NIST and ISO have played a crucial role in the development and adoption of cryptographic standards, ensuring interoperability and security across different systems and applications. These standards provide guidelines for implementing secure cryptographic algorithms and protocols, which are essential for protecting sensitive information in various domains.

Cryptography now underpins modern technologies such as blockchain, digital currencies, secure messaging applications, and the Internet of Things (IoT). Blockchain technology, for instance, relies on cryptographic hashing and digital signatures to ensure the integrity and authenticity of transactions. Similarly, end-to-end encryption in messaging apps like Signal and WhatsApp ensures that only the intended recipients can read the messages.

The field has also had to evolve to counter various cryptographic attacks, including side-channel attacks, brute force attacks, and sophisticated cryptanalysis techniques. Researchers continually

develop new defenses and cryptographic primitives to enhance the security of digital systems and protect against these evolving threats.

Looking to the future, emerging trends in cryptographic research include advancements in homomorphic encryption, which allows computations on encrypted data without decrypting it; zero-knowledge proofs, which enable the verification of a statement without revealing any information beyond its truth; and quantum key distribution, which uses the principles of quantum mechanics to securely distribute cryptographic keys.

3 The Cypherpunk Manifesto: A Political Declaration

In the book, *Cypherpunk: Privacy and Security in the Digital Age* [3], Anderson addresses several issues concerning the ethics and manifesto of the cypherpunk movement from an updated philosophical perspective since the book is relative new and it has a modern approach about cypherpunk moviment and ethics.

> "Yet, cypherpunk philosophy is about more than the politics of security and privacy. At its roots, the cypherpunk worldview is fundamentally normative, which means it is built upon claims about what people and institutions *ought to do* and what societies *ought to be like*." [3]

This citation allows us to draw a correlation with the anarchist movement and even infer that cypherpunk philosophy can be viewed as a digital iteration of anarchism. A parallel can be made with an earlier work by Bakunin, which echoes similar normative claims about society:

> "We are convinced that freedom without Socialism is privilege and injustice, and that Socialism without freedom is slavery and brutality." [4]

Both quotes highlight a fundamental belief in how societies should be structured and the importance of balancing freedom and justice. While Anderson's cypherpunk philosophy emphasizes digital privacy and security, Bakunin's anarchism underscores the need for societal freedom and equality. Together, they reflect a shared vision of normative principles guiding societal ideals. This raises a natural question for the cypherpunk movement: "Is this the guide for digital society?"

As previously mentioned, we must recognize that the distinction between the "real" world and the "digital" world is becoming increasingly blurred. Therefore, another pertinent question is: "Should we update our views on cryptographic constructions to reflect this unified reality?"

The Cypherpunk Manifesto posits that cryptography is a fundamental tool for protecting privacy and fostering individual freedoms in the digital age. Key tenets of the manifesto include:

- **Privacy as a Fundamental Right**: Asserting that privacy is essential for a free society and that individuals must have the means to protect their personal information. This right to privacy is seen as a cornerstone for other civil liberties, emphasizing that without privacy, other freedoms are significantly undermined.
- **Decentralization and Individual Empowerment**: Emphasizing the importance of decentralized systems and empowering individuals through the use of strong cryptography. Decentralization is crucial to preventing abuses of power by centralized authorities, thereby fostering a more resilient and equitable digital ecosystem.

– **Activism and Practical Application**: Encouraging the development and deployment of cryptographic tools by activists to counteract government and corporate surveillance. This activism is rooted in the belief that practical, technological solutions are necessary to preserve freedom in the digital age, where legislative measures alone may fall short.

In the modern world, where digital and physical realities are intertwined, the principles of the Cypherpunk Manifesto are more relevant than ever. Cryptography is not just a tool for securing information but a foundational element for ensuring personal autonomy and resisting oppressive structures. As technology continues to evolve, the manifesto's call for privacy, decentralization, and proactive activism provides a crucial framework for building a fair and just digital society.

4 Ethical Responsibilities of Cryptographers

In his paper, *The Moral Character of Cryptographic Work* [10], Phillip Rogaway argues that cryptographic research is not value-neutral and that cryptographers have a moral responsibility to consider the social and political implications of their work. He makes several key points:

– **Ethical Responsibility**: Cryptographers should recognize their ethical responsibility and the impact their work can have on society.
– **Historical Context**: The development of cryptography has been deeply intertwined with governmental and military interests, particularly in surveillance and intelligence gathering.
– **Surveillance and Control**: Modern cryptographic work often indirectly supports systems of surveillance and control, which can conflict with the values of privacy and civil liberties.
– **Public Good**: Cryptographers should aim to contribute to the public good, developing technologies that protect individuals' privacy and resist authoritarianism.
– **Political Engagement**: Rogaway encourages cryptographers to be politically engaged and to consider the broader societal implications of their research.

Rogaway advocates for a paradigm shift in cryptography, urging researchers to adopt a more socially conscious approach. This entails not only focusing on technical aspects but also actively engaging in discussions about the ethical and political dimensions of their work.

Despite Rogaway's influential publication, little has changed regarding ethical challenges in academic cryptography. This includes the International Association for Cryptologic Research (IACR), which remains deficient in formal ethical guidelines.

Cryptography is inherently multidisciplinary, prompting questions about its ethical foundations—whether rooted in mathematics, computer science, or engineering. Karst and Slegers [8] highlight the varied integration of ethics across departments offering cryptography education, underscoring the need for cohesive ethical standards.

Comparatively, some departments exhibit more explicit ethical frameworks than others. For instance, the Association for Computing Machinery (ACM) upholds detailed codes of ethics and professional conduct, including directives on honesty, privacy, and societal contribution [1]. In contrast, the American Mathematical Society (AMS) and Mathematical Association of America (MAA) provide more generalized guidance on ethical conduct [2,9]. In fact, we can say that the professional codes only briefly (and very vaguely) touch on issues related to ethics:

> "The MAA requires Directors, Officers, Members, those compensated by the MAA and those donating their time, and all employees to observe high standards of business and personal ethics in the conduct of their duties and responsibilities." [9]

> "When mathematical work may affect the public health, safety or general welfare, it is the responsibility of mathematicians to disclose the implications of their work to their employers and to the public, if necessary." [2]

Notably, the Society for Industrial and Applied Mathematics (SIAM) lacks a formal code of ethics. Another important institution for cryptography, the IACR, despite its focus on cryptography, similarly lacks a comprehensive ethical statement[1]. This gap is striking given the profound intersection of cryptography with political and societal issues.

Philosophical Discussion on Ethics

Defining ethics is a challenging task due to its philosophical nature and varied interpretations in literature. Ethics deals with questions about morality, values, right and wrong behavior, and principles guiding individual or collective conduct. It examines what constitutes good and bad behavior, how individuals should act in various situations, and the reasons behind moral judgments [11].

As a community rooted in mathematics and computer science, the cryptographic community values precision in definitions and rigorous reasoning. However, moral reasoning offers a pathway towards a more formal definition. It involves constructing arguments supported by sound reasons and conclusions, aiming for both accuracy and logical coherence.

> "Our moral thinking should have two complementary goals: getting it right, and being able to back up our views with flawless reasoning. We want the truth, both in the starting assumptions we bring to an issue and in the conclusions we eventually arrive at. But we also want to make sure that our views are supported by excellent reasons. And this provides two tests for good moral reasoning: first, we must avoid false beliefs, and second, the logic of our moral thinking must be rigorous and error-free." [11, Ch. 1, Page 10]

The debate on the morality of cryptographic work centers around the balance between advancing technological capabilities and addressing the ethical consequences of such advancements. Cryptographers must navigate complex ethical terrains where their work could both protect individual privacy and enable surveillance. The moral character of cryptographic work demands a reflective approach, considering how cryptographic tools and techniques impact societal norms and values. This debate is not merely academic but has real-world implications, influencing policy decisions and shaping the future of privacy and security in the digital age. Addressing these ethical concerns requires an ongoing dialogue between technologists, ethicists, policymakers, and the public to ensure that cryptographic advancements align with the broader societal good.

In other words, the absence of a code of conduct and ethics in the field could undermine its future growth, especially as it attracts more scientists from diverse backgrounds and age groups. We cannot assume that everyone will inherently adhere to the field's ethical standards. However, establishing clear ethical guidelines can ensure more precise and consistent statements from an academic association, aligning its bylaws with the broader principles of scientific integrity and morality.

[1] Data retrieved from `https://www.iacr.org/docs/`

5 Cryptography, Anarchism and the Future

As mentioned in Section 3, the Cypherpunk Manifesto and anarchism exhibit significant similarities. The relationship between cryptography and anarchism is *rooted in their shared emphasis on privacy, individual freedom, and resistance to centralized control.* Key points of intersection include:

- **Privacy and Individual Autonomy**: Anarchists advocate for individual autonomy and personal privacy, opposing any form of coercion or surveillance by the state or other centralized authorities. Cryptographic technologies enable individuals to maintain their privacy and autonomy in the digital age.
- **Resistance to Centralized Control**: Anarchism opposes centralized control and hierarchical structures, advocating for decentralized and voluntary associations. Cryptography supports decentralized systems by enabling secure peer-to-peer communications and transactions without relying on centralized authorities.
- **Empowerment of Individuals**: Anarchists aim to empower individuals by dismantling oppressive systems and enabling self-governance and mutual aid. Cryptographic tools empower individuals to protect their own data and communications, giving them control over their digital presence and interactions.
- **Anonymity and Pseudonymity**: Anonymity can be a tactic for anarchists to protect themselves from state repression and to organize without fear of retaliation. Cryptographic techniques, such as Tor and anonymous cryptocurrencies, provide anonymity and pseudonymity, allowing individuals to operate without revealing their identities.
- **Philosophical Underpinnings**: The philosophical underpinnings of anarchism include a strong belief in personal liberty, non-coercion, and skepticism towards authority. The cypherpunk movement, which champions the use of cryptography to achieve privacy and security, shares similar philosophical values.
- **Historical Context**: Throughout history, anarchists have often used secret communication methods to avoid detection and repression. The development of modern cryptographic techniques has been partly motivated by the desire to protect individuals and groups from oppressive regimes.

From these key points, it is evident that cryptography serves as a crucial tool to achieve various anarchist objectives. Cryptographic methods have been tailored to meet specific needs within the anarchist framework, such as ensuring secure communication channels, protecting the identities of activists, and facilitating decentralized coordination. By enabling private and secure interactions, cryptography helps anarchists resist surveillance and maintain operational security. This technological empowerment allows for the practical application of anarchist principles, fostering environments where decentralized and voluntary associations can thrive without external interference.

However, in recent years, the values that once underpinned cryptographic development seem to have been overshadowed by a focus on financial gain. The rise of cryptocurrencies, while initially aligned with ideals of decentralization and financial autonomy, has increasingly become dominated by speculative interests and profit motives. This shift towards monetization risks undermining the ethical foundations of cryptography, diverting attention away from its potential to protect privacy and empower individuals. The community must remember the original values articulated by the cypherpunks and strive to balance innovation with ethical considerations, ensuring that the pursuit of profit does not eclipse the commitment to privacy and individual freedom.

Cryptography has undergone significant changes since the introduction of the Diffie-Hellman key exchange protocol. Initially, cryptography was a highly academic and scientific field focused on theoretical advancements and the pursuit of knowledge. However, over time, it has evolved into a commercial enterprise, with companies leveraging cryptographic technologies to develop and sell products. This commercialization has shifted the focus from academic inquiry to market-driven solutions, often prioritizing profit over the ethical and scientific values that originally guided the field. It is crucial for the cryptographic community to reclaim its academic roots and reaffirm its commitment to scientific rigor and ethical responsibility. We need to refocus on several key academic aspects of cryptography. While the standardization process and secure implementations are important, should they consume all our attention? What happened to exploring new attacks and developing alternative cryptographic schemes?

The intersection of cryptography and anarchism reveals a profound alignment in their core values of privacy, individual freedom, and resistance to centralized control. By exploring these connections in detail, we can better understand the role of cryptographic technologies in advancing these principles and addressing the ethical challenges that arise. The continued dialogue and collaboration between technologists, ethicists, and activists will be crucial in ensuring that cryptographic advancements contribute to a freer and more just society.

Another critical point is the increasing distance between academic focus and the notion of "non-profit" within our field. Should our primary goal not be the advancement of knowledge? When did we lose our focus and allow large tech companies to dominate our conferences? For instance, how can a student without substantial funding afford to attend a conference in a city like Zurich, with registration fees around 450 euros, plus hotel and travel costs? While stipends offer a partial solution, would it not be better to choose more affordable locations to let a broader participation? When did we become so elitist that we cannot hold conferences in less well-known but more economical cities? This shift towards high-cost venues limits accessibility and inclusivity, contrary to the foundational values of academic and scientific inquiry.

References

1. ACM. Acm code of ethics and professional conduct.
2. American Mathematical Society (AMS). Ethical guidelines of the american mathematical society. http://www.ams.org/about-us/governance/policy-statements/sec-ethics, 2024. [Online; accessed 10-May-2024].
3. Patrick D Anderson. *Cypherpunk ethics: Radical ethics for the digital age*. Routledge, 2022.
4. Mikhail Bakunin. Federalism, socialism, anti-theologism. *Bakunin on Anarchy: Selected Works by the Activist-Founder of World Anarchism*, pages 102–147, 1867.
5. David Chaum. Security without identification: Transaction systems to make big brother obsolete. *Communications of the ACM*, 28(10):1030–1044, 1985.
6. Whitfield Diffie and Susan Landau. *Privacy on the Line: The Politics of Wiretapping and Encryption*. MIT Press, 2001.
7. Eric Hughes. A cypherpunk's manifesto, 1993.
8. Nathaniel Karst and Rosa Slegers. Cryptography in context: co-teaching ethics and mathematics. *PRIMUS*, 29(9):1039–1059, 2019.
9. Mathematical Association of America (MAA). Welcoming environment, code of ethics, and whistleblower policy. http://www.maa.org/about-maa/policies-and-procedures/welcoming-environment-code-of-ethics-and-whistleblower-policy, 2024. [Online; accessed 10-May-2024].
10. Phillip Rogaway. The moral character of cryptographic work, 2015.
11. Russ Shafer-Landau. *The fundamentals of ethics*. Oxford University Press, 4 edition, 2018.