Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

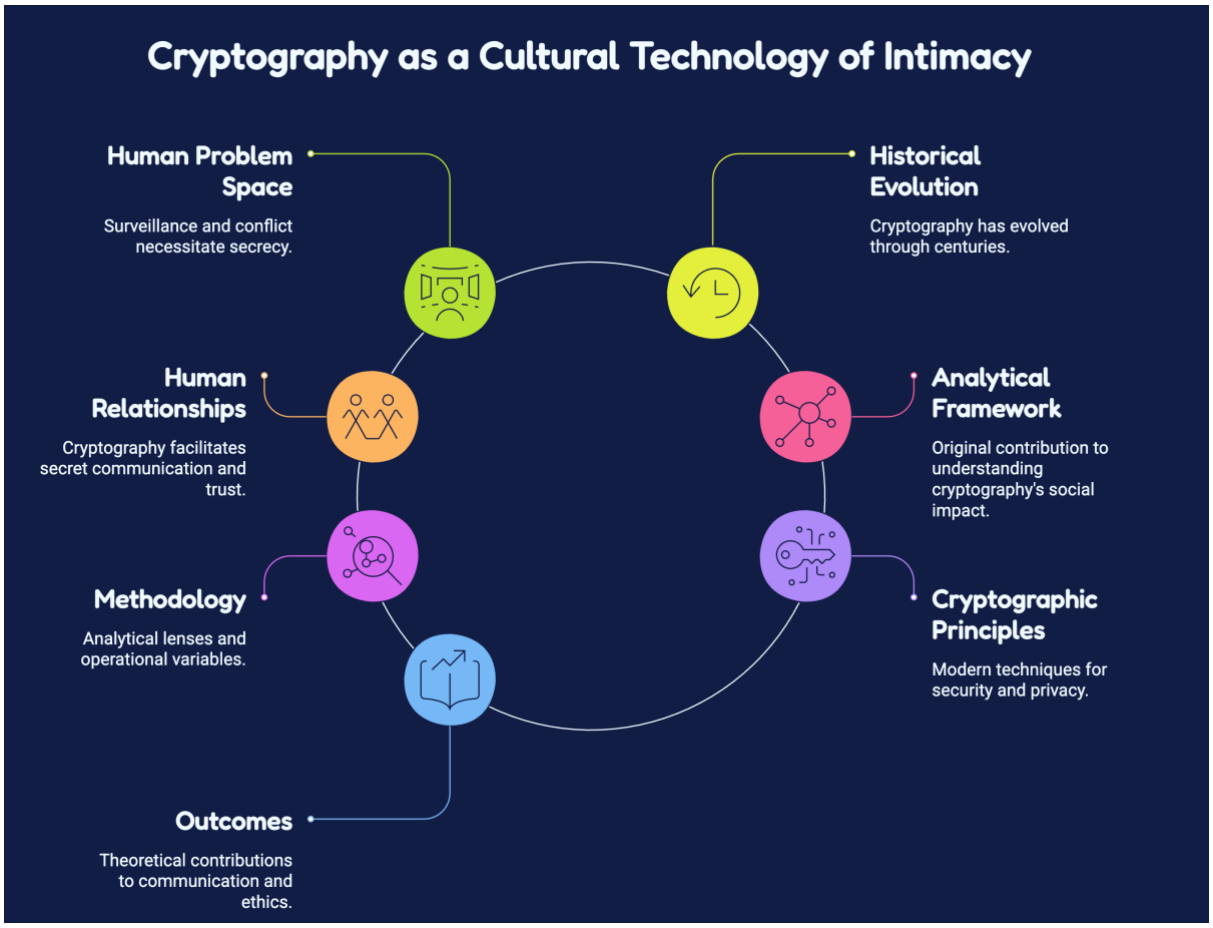
Link to the published article: https://doi.org/10.3389/fhumd.2026.1716741

Full reference: Radanliev, Petar, "Cryptography, romance, and war," *Frontiers in Human Dynamics*, vol. 8, p. 1716741, Jul. 2026, doi: 10.3389/FHUMD.2026.1716741, URL: https://www.frontiersin.org/articles/10.3389/fhumd.2026.1716741/full

Cryptography, Romance, and War

Dr Petar Radanliev

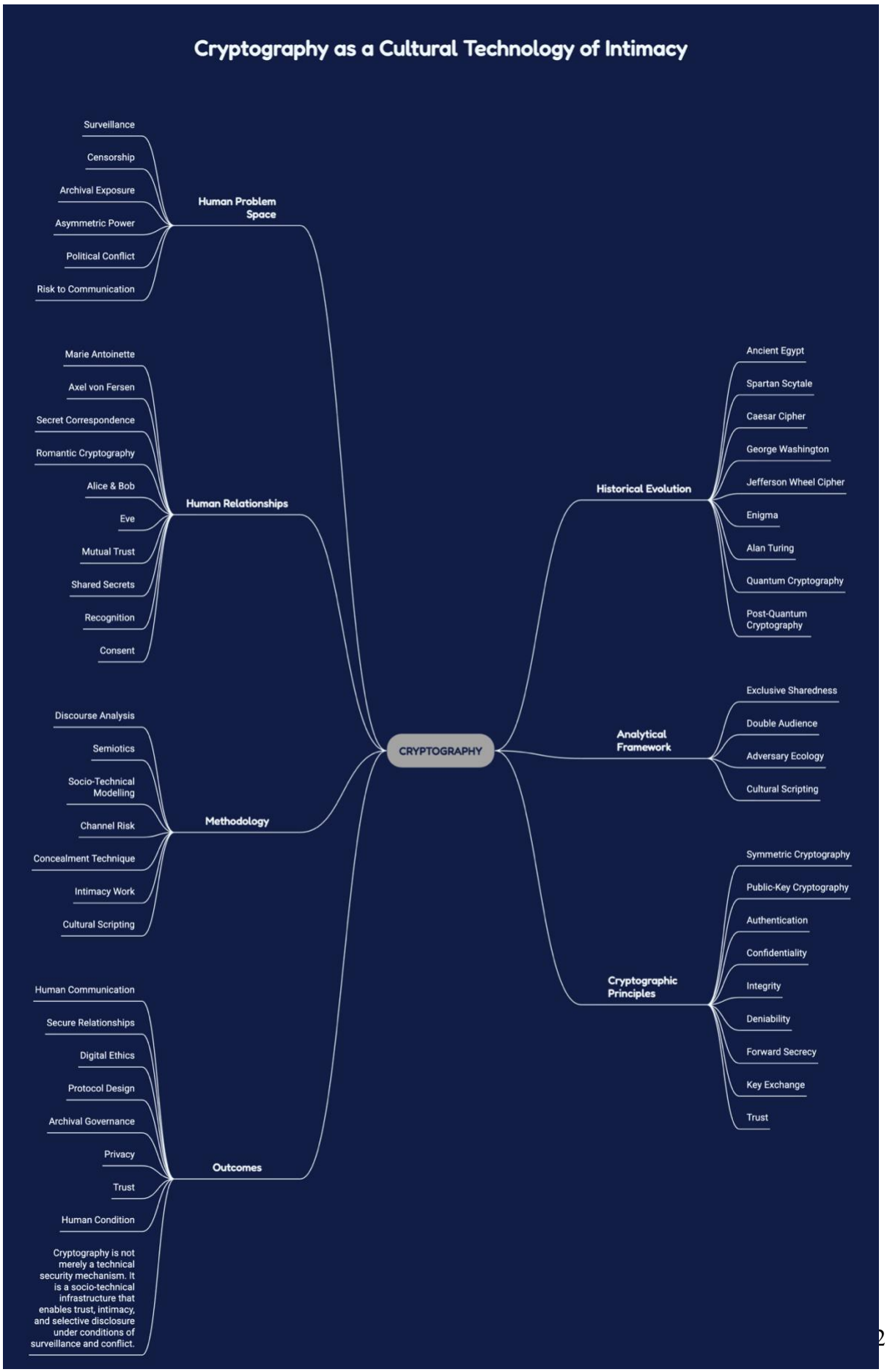
Department of Computer Sciences, University of Oxford, Wolfson, Building, Parks Rd, Oxford OX1 3QG, Email: petar.radanliev@cs.ox.ac.uk



Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

UNIVERSITY OF OXFORD

DEPARTMENT OF COMPUTER SCIENCE



Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

Research IDs:
ORCID: https://orcid.org/0000-0001-5629-6857
ResearcherID: L-7509-2015
ResearcherID: M-2176-2017
Scopus Author ID: 57003734400
Loop profile: 839254
ResearcherID: L-7509-2015

Abstract:

Introduction: Cryptography is conventionally understood as a technical mechanism for securing information against adversaries. This article advances a complementary claim: that cryptography functions as a socio-technical and cultural technology for sustaining intimate communication under conditions of surveillance, censorship, archival exposure, and asymmetric power. The study asks how cryptographic techniques have historically enabled intimacy to persist where disclosure would entail personal, political, or existential risk.

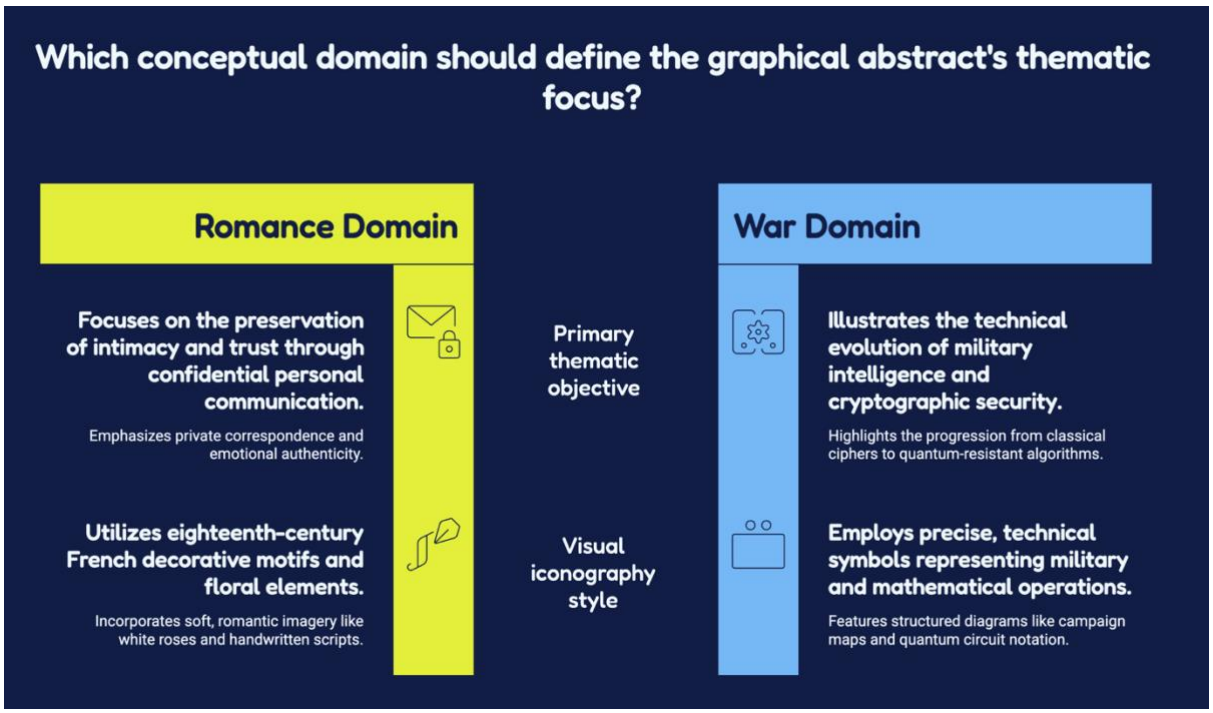
Methods: The analysis integrates three corpora, archival love correspondence, literary representations of hidden writing, and mythic narratives of sanctioned secrecy, using discourse analysis, semiotics, and socio-technical modelling. A historical case study of the encrypted correspondence between Marie Antoinette and Axel von Fersen is examined alongside formal abstractions from modern cryptography. Analytical variables capturing channel risk, concealment technique, intimacy work, and cultural scripting are operationalised to derive testable propositions.

Results: The study develops a four-component model of cryptographic intimacy, Exclusive Sharedness, Double Audience, Adversary Ecology, and Cultural Scripting, and articulates five propositions explaining how secrecy practices adapt to risk, coordination cost, temporal ethics, and power asymmetry. These patterns recur across historical, literary, and technical domains as structured responses to threats against intimacy.

Discussion: Reframing cryptography as a cultural technology of intimacy shows how cryptographic design formalises human predicates such as recognition, consent, deniability, and temporally bounded trust. The findings have implications for protocol design, archival governance, and digital ethics, positioning cryptography as integral to the human condition rather than solely to information security.

Keywords: cryptography; intimacy and the human condition; socio-technical systems; secrecy and surveillance; archival exposure; cultural technology; science and technology studies; discourse and semiotic analysis; power asymmetry; digital ethics.

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate



Introduction

Cryptography is conventionally understood as a technical infrastructure for confidentiality, authentication, and secure communication. Yet historically, cryptographic practices have also functioned as mechanisms for sustaining intimacy under conditions of surveillance, censorship, coercion, and archival exposure. Across romantic correspondence, wartime communication, literary representation, and modern digital systems, secrecy repeatedly emerges not merely as a defensive technical property, but as a socio-technical condition for trust, vulnerability, recognition, and selective disclosure. This article develops an interdisciplinary framework that reconceptualises cryptography as a cultural technology of intimacy. Rather than treating secrecy solely as a mathematical or computational problem, the paper examines how cryptographic practices encode relational structures shaped by power asymmetry, adversarial observation, and temporally bounded trust.

This article addresses the following research question: How have cryptographic techniques historically functioned as socio-technical mechanisms for sustaining intimate communication under conditions of surveillance, conflict, and asymmetric power, and what design principles can be abstracted from these practices? The analytical structure of the paper is organised around the claim that cryptography emerges as a response to concrete risks facing intimate communication under conditions of surveillance, censorship, archival exposure, and asymmetric power. Figure 3 provides an overview of this structure by situating the core model of cryptography as a cultural technology of intimacy between the contextual problem space and the paper's principal findings.

The scope of the paper is deliberately constrained to cryptography as a *relational technology*, rather than as a comprehensive survey of security mechanisms. The analysis focuses on intimate communication, particularly romantic correspondence, not because such cases are exceptional, but because they expose, in concentrated form, the human predicates that

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

cryptography formalises: selective disclosure, recognition, consent, deniability, and temporally bounded trust.

War, censorship, and state surveillance are treated as boundary conditions that intensify communicative risk, thereby rendering cryptographic practices analytically visible. Technical mechanisms are discussed only insofar as they illuminate how secrecy operates as social labour within these constrained environments. Topics that do not directly contribute to this analytical frame are excluded or treated only as illustrative boundary cases. All subsequent sections are organised to address this research question directly, either through historically situated case analysis, formal abstraction, or analytically bounded counter-examples.

The four-component model of cryptographic intimacy introduced in this paper, Exclusive Sharedness, Double Audience, Adversary Ecology, and Cultural Scripting, serves as the primary analytical spine of the manuscript. All subsequent sections are organised to elaborate, instantiate, or test this model across historical, formal, and contemporary cases, ensuring conceptual continuity and avoiding thematic drift.

The paper proceeds in seven stages. First, it situates the study within existing scholarship on privacy, socio-technical systems, and cryptographic imaginaries. Second, it develops the methodological framework and operational variables guiding the analysis. Third, it introduces the conceptual framework of cryptography as a cultural technology of intimacy. Fourth, it examines the Marie Antoinette–Fersen correspondence as a historically situated case of intimate secrecy under surveillance. Fifth, it compares this historical material with formal abstractions in modern cryptography, particularly the Alice–Bob adversarial model. Sixth, it analyses how contemporary cryptographic architectures encode competing assumptions about secrecy, accountability, and archival permanence. Finally, the paper discusses the implications of these findings for cryptographic design, digital ethics, and socio-technical governance.

Methodology

This study adopts an interdisciplinary mixed-methods design integrating qualitative discourse analysis, semiotic interpretation, and socio-technical modelling. The methodological objective is not statistical generalisation but analytical abstraction: identifying recurring structural relationships between secrecy practices, communicative risk, and relational intimacy across heterogeneous corpora. The study therefore combines interpretive qualitative analysis with formal analytical modelling to derive operational variables and testable propositions regarding cryptographic behaviour under adversarial conditions.

Data Selection and Corpus Construction

The analysis draws on three primary corpora:

1. Archival intimate correspondence produced under conditions of surveillance, censorship, or political risk.
2. Literary representations of concealed writing, cryptographic signalling, and dual-audience communication.
3. Mythic and symbolic narratives involving ritualised secrecy, hidden knowledge, or communicative restriction.

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

The Marie Antoinette–Fersen correspondence serves as the principal historical case study because it combines high emotional stakes, institutional surveillance, archival preservation, and demonstrable cryptographic techniques within a single corpus. Literary and mythic materials are not treated as empirical evidence equivalent to archival records; rather, they are analysed as cultural artefacts that reveal how secrecy and intimate communication are socially imagined, narrated, and ritualised.

Selection criteria prioritised materials in which:

- communicative risk was explicitly present;
- concealment techniques were observable;
- and secrecy functioned relationally rather than purely strategically.

The corpus is intentionally interdisciplinary and analytically bounded rather than historically exhaustive.

Methods and Analytical Procedure

The methodological framework integrates three complementary analytical approaches.

Discourse analysis is used to examine how secrecy, concealment, recognition, and vulnerability are linguistically constructed within textual materials. Particular attention is given to euphemism, omission, ambiguity, and dual-audience communication.

Semiotic analysis examines how symbolic concealment generates layered meaning beyond literal inscription. Redactions, coded references, erased passages, ritualised symbols, and contextual markers are interpreted as communicative signs whose meaning depends on shared interpretive frameworks.

Socio-technical modelling abstracts recurring patterns from the historical and textual materials into operational variables and propositions. This stage maps communicative practices onto cryptographic concepts including adversarial models, selective disclosure, deniability, authentication, and temporally bounded trust.

Strengths and Limitations

The principal strength of this methodology lies in its ability to bridge technical cryptography, historical analysis, and socio-technical theory within a single analytical framework. By integrating formal cryptographic concepts with archival and cultural materials, the study identifies structural continuities that are often obscured by disciplinary boundaries.

The methodology is nevertheless subject to important limitations. The corpus is predominantly Western and archival, reflecting both historical preservation biases and the availability of documented encrypted correspondence. Literary and mythic materials necessarily involve interpretive subjectivity and are therefore used analytically rather than evidentially. The study also does not claim empirical representativeness across all cryptographic practices or cultural traditions.

The propositions advanced in this paper are therefore intended as analytically generalisable rather than statistically universal. Future research could extend the framework to non-Western corpora, digital communication platforms, and ethnographic studies of contemporary encrypted intimacy.

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

UNIVERSITY OF OXFORD
DEPARTMENT OF COMPUTER SCIENCE

Ethical Considerations

The study relies exclusively on publicly accessible archival, literary, and historical materials and does not involve living participants, private datasets, or personally identifiable contemporary communications. Nevertheless, the analysis recognises that intimate correspondence raises ethical questions regarding retrospective exposure, archival interpretation, and the politics of disclosure.

The paper therefore treats secrecy not merely as an object of analysis but as an ethical condition shaped by consent, vulnerability, and power asymmetry. This ethical orientation directly informs the paper's treatment of archival exposure, deniability, and temporally bounded trust within the broader framework of cryptographic intimacy.

Literature Review: Cryptography, Secrecy, and Socio-Technical Intimacy

Cryptography, at its core, it addresses three functional requirements: confidentiality (preventing unauthorised access to content), integrity (detecting unauthorised modification), and authentication (verifying the identity of communicating parties) (Katz and Lindell, 2014). Cryptography is derived from the Ancient Greek words kryptós "hidden, secret"; and γράφειν "to write", or -λογία -logia, "study", implying it is the study of secure and hidden writing (Buchmann, 2004a). It is fundamentally the science of encoding and decoding information to protect it from unauthorised access (Hoffstein, Pipher and Silverman, 2014). Cryptography is crucial for secure communication (Delfs, Knebl and Knebl, 2002), especially in the presence of malicious third parties (Buchmann, 2004b), known as adversaries. It involves two main processes: encryption, where data is converted into a secret code, and decryption, where the secret code is converted back to its original form (Mollin, 2006). This field has evolved to include a variety of techniques and types, such as Secret Key Cryptography, which ensures the confidentiality, integrity, and authenticity of information (Vaudenay, 2005).

Methodological and analytical scope

Cryptography is conventionally framed within computer science, information security, and applied mathematics as a formal mechanism for achieving confidentiality, integrity, authentication, and non-repudiation in the presence of adversaries (Oded 2009; Katz and Lindell 2014). Within this paradigm, cryptographic research prioritises provable security under defined threat models, computational hardness assumptions, and protocol correctness. Foundational formulations (Diffie and Hellman 1976; Rivest et al. 1978; Chaum 1981), explicitly conceptualise cryptography as enabling private communication between parties over insecure channels. Even in early privacy-enhancing visions (Chaum 1983), the emphasis remains on secure communication infrastructures rather than on the relational, affective, or cultural dimensions of secrecy.

This dominant framing is not incorrect; however, it is analytically incomplete. While cryptography is studied as a subfield of cybersecurity and formal systems design, it simultaneously operates as a socio-technical practice embedded in relationships, institutions, and power structures. Science and Technology Studies scholarship has begun to interrogate the social imaginaries surrounding encryption (West 2018), the politics of trust in

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

cryptographic systems (Balsa et al. 2022), and the contextual integrity of information flows (Nissenbaum 2004, 2009). Yet cryptography itself remains primarily theorised as a defensive infrastructure rather than as a cultural technology through which intimacy, vulnerability, and recognition are structured. This article intervenes precisely at that juncture.

This article advances the claim that cryptography functions as a socio-technical infrastructure for intimacy: it enables private bonds to persist under conditions of surveillance, coercion, and unequal power. Romantic correspondence provides a particularly revealing empirical site, because it combines high emotional stakes with high communicative risk. The necessity to conceal affection, identity, or intent foregrounds the same design problems addressed by formal cryptographic systems: who may know what, when, and under which conditions.

Rather than offering a chronological history of cryptographic techniques, the paper develops an analytical framework for understanding how secrecy operates across historical correspondence, literary representation, and mythic narrative. These domains are examined not as anecdotal curiosities, but as structured environments in which cryptographic reasoning, albeit often informal or non-mathematical, emerges in response to censorship, interception, and archival exposure.

The contribution of this work lies in articulating a four-component model of cryptographic intimacy, Exclusive Sharedness, Double Audience, Adversary Ecology, and Cultural Scripting, and in demonstrating how this model accounts for both historical practices of concealed communication and contemporary protocol design choices. In doing so, the article situates cryptography within the broader field of human dynamics and digital impacts, treating secrecy as a foundational mechanism through which trust, vulnerability, and social power are negotiated.

A fundamental distinction is drawn between symmetric and asymmetric cryptography. Symmetric cryptography relies on a single shared secret key used for encryption and decryption. Its historical antecedents include substitution and transposition ciphers, while modern implementations include block and stream ciphers such as AES. Symmetric systems are computationally efficient but require secure key distribution, a constraint that becomes salient in hostile or surveilled environments. Asymmetric (public-key) cryptography employs mathematically linked key pairs: a public key for encryption or verification, and a private key for decryption or signing. This asymmetry enables secure communication without prior secret sharing and formalises concepts of recognition, consent, and accountability. In the context of intimate communication, public-key cryptography is analytically significant because it models selective accessibility rather than absolute secrecy. This distinction underpins the analytical framework of this paper: different cryptographic forms embody different social solutions to the problem of communicating under risk.

The strength of cryptographic algorithms is directly proportional to the difficulty of mathematical problems they pose. For instance, the RSA public-key encryption algorithm (Rivest, Shamir and Adleman, 1978) is founded on the challenge of factoring the product of two large prime numbers. If intruders solve this mathematical hurdle, they can access the encrypted data. A large-scale quantum computer could easily crack the current cryptographic algorithms. Symmetric algorithms, such as AES (Daemen and Rijmen, 2003) and Blowfish, demand that the secret key remains confidential. Any vulnerability in the implementation, such as insecure key storage or transmission, could expose the secret key, thereby putting the security of the encrypted data at risk. Throughout history, cryptography has been used in

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

warfare to ensure secure communication and safeguard confidential information from being intercepted by the enemy. A prominent example of cryptography employed during World War II is highlighted in novels like Neal Stephenson's "Cryptonomicon" (Stephenson 1999), which emphasises the significance of cryptography in modern-day and wartime scenarios. Fictional works referencing cryptography are treated in this paper solely as conceptual artefacts that reflect cultural understandings of secrecy, trust, and communication under threat. They are not used as historical evidence for cryptographic practice, but as narrative environments in which cryptographic logics are imaginatively explored and socially interpreted.

This paper does not equate cryptography with cybersecurity. The distinction is introduced solely to delimit analytical scope. Cybersecurity concerns the protection of systems, networks, and infrastructures, whereas cryptography concerns the properties of communication itself. The present analysis isolates cryptography because intimacy, secrecy, and selective disclosure operate at the level of communicative exchange rather than system defence. No further claims are made regarding cybersecurity practice. Historical treatments of cryptography draw on established scholarship in classical, medieval, and early modern cryptographic practices, including Kahn (Kahn, 1996), Singh (Singh, 2011), and Barker (Barker, 2020). Quantum cryptographic discussions reference foundational work by Bennett and Brassard (Bennett and Brassard, 2014a), Shor (Shor, 1994; 1997), and contemporary post-quantum surveys (Bernstein, Buchmann and Dahmn, 2010). This manuscript is structured around public-key cryptography as the primary formal exemplar, with historical cases treated as structurally homologous antecedents rather than as chronological survey material.

Historical Cryptography and Adversarial Communication

Cryptographic practices have existed across historical periods, but their form, function, and guarantees differ fundamentally from modern cryptography. Ancient techniques such as the Spartan scytale, Roman substitution ciphers, and Egyptian non-standard hieroglyphs relied on obscurity, limited literacy, and controlled circulation. Their security assumptions were social and material rather than computational.

Modern cryptography, by contrast, is defined by mathematically formalised threat models, algorithmic hardness assumptions, and explicit adversary capabilities. The historical relevance of cryptography therefore lies not in technical equivalence, but in functional continuity: across periods, cryptographic techniques arise where communication must persist under surveillance, coercion, or rivalry.

The earliest recorded instance of encryption dates to 1900 BC in ancient Egypt, where hieroglyphs were utilised to encode messages. Throughout history, encryption has been a crucial tool in transmitting secret messages. The ancient Greeks created their own encryption device called the scytale, which involved wrapping a strip of cloth around a stick. During the Roman Empire, Julius Caesar used encryption to cipher his letters and communications. Encryption has been widely used in military circles and is an important asset in many battles. The enigma (Figure 1) was a cipher machine that Nazi

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

Germany's military command used to encode strategic messages before and during World War II.

Figure 1: Variants of the machine, used by Germany's military and civil authorities from the late 1920s through World War II, implemented a complex electro-mechanical polyalphabetic cipher.

Historical cryptographic practices across ancient Egypt, Greece, Rome, early modern Europe, and twentieth-century warfare reveal a persistent functional continuity: secrecy emerges wherever communication must survive hostile observation. Although the technical sophistication of these systems differs substantially from contemporary cryptography, their social logic remains comparable. Substitution ciphers, concealed writing, coded correspondence, and wartime encryption all reflect attempts to manage adversarial visibility, selective disclosure, and asymmetrical access to information. Existing historical scholarship has extensively documented these developments (Kahn 1996; Singh 2011), yet such work typically treats cryptography as an evolving technical discipline rather than as a socio-technical practice of relational protection and communicative survival."

Ancient Egypt - the use of 'hieroglyph'

Apart from Ancient Greece, the origins of cryptography can be traced back to approximately 1900 BC in ancient Egypt, where it was used to protect and transfer covert messages. The Egyptians, known for their advanced writing system, utilised non-standard hieroglyphs to encode messages. This practice was most likely used to protect confidential information or to secretly transmit messages, possibly concerning military strategy or diplomatic communications.

During ancient Egyptian times, the context of war and conflict required the development of secure communication methods. Cryptography was likely essential in maintaining the security of military strategies and state secrets. This allowed pharaohs and military leaders to communicate without fear of interception by adversaries. The encrypted messages may have contained vital information about troop movements, battle plans, and alliances. All of these were crucial for gaining a strategic advantage in conflicts.

It is believed that ancient Egyptian warfare used cryptography to conceal information. The use of non-standard hieroglyphs indicates a deliberate effort to keep messages secret. This practice of information concealment laid the foundation for developing cryptography as a scientific discipline. It reflects humanity's need for secure communication during war and peace.

Cryptography during ancient Egypt formed a critical part of the strategic arsenal of the ancient Egyptian civilisation, enabling the secure transfer of sensitive data and playing a key role in shaping military and political landscapes. The importance of cryptography in ancient Egypt highlights its function to protect confidential information and an enable covert activities.

Ancient Greece – the Scytale

The ancient Greeks used a scytale, in which the person sending a message wound a strip of cloth around a stick. During the time of ancient Greece, the Scytale was a coveted cryptographic device that played a pivotal role in maintaining secure communication. It

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

functions as a transposition cipher by enveloping a strip of parchment around a cylindrical object and inscribing the message across it. Once unfurled, the parchment displays a sequence of seemingly unconnected characters that can only be decoded with a cylinder of matching dimensions. Despite its apparent simplicity, the Scytale remains a remarkably ingenious and successful encryption technique that has endured through the ages.

During military operations, the Spartan military relied on the Scytale as a tool to maintain the secrecy of sensitive information. This device was a testament to the Spartans' ingenuity and dedication to ensuring the safety of their communications. The Scytale employed cryptographic principles to implement a sophisticated encryption and coding system that provided a strategic approach to secure communication during wartime. The encryption and coding system used by the Scytale made it difficult for enemies to intercept and decode sensitive military information. The Scytale was a vital tool that played a crucial role in the success of Spartan military operations, and it remains an important artefact that reflects the advanced knowledge and skills of the Spartan civilisation.

In today's military, the effectiveness of communication channels is critical to successful operations. Modern military strategies have come to rely on advanced cryptographic methods to ensure the secure transmission of information. Interestingly, the foundation for these methods can be traced back to an ancient tool known as the Scytale. By using principles of transposition and substitution ciphers, the Scytale laid the groundwork for modern cryptographic algorithms that have been instrumental in protecting communication channels for military operations and ongoing war efforts.

From ancient times to modern strategic missions, the Scytale has played a role in cryptography. This tool has been used to ensure the confidentiality of transmitted messages, emphasising the importance of keeping sensitive information from falling into the wrong hands. Its use has enabled military personnel to communicate without fear of interception or decoding by enemies, allowing for more effective and efficient communication in the most critical of situations.

Ancient Rome – The Caesar Cipher

The Caesar Cipher is a substitution cipher that traces its roots to Ancient Rome and is attributed to Julius Caesar. He relied on this technique to encrypt his military communications. This cryptographic method is significant since it underscores the relationship between the key and algorithm, which are fundamental principles in cryptography.

The Caesar Cipher, also known as a "shift cipher," operates by utilising a simple shifting mechanism. Each letter in the original message is replaced with a corresponding letter in the alphabet fixed to it. The key, or shift value, determines the displacement between the letters. For example, with a shift of 1, 'A' becomes 'B,' 'B' becomes 'C,' and so on. This method ensures that the original message, or plaintext, is transformed into an unintelligible string of characters known as ciphertext.

To employ the Caesar Cipher for encrypting a message, begin by selecting a shift value. Next, substitute each letter in the plaintext with the letter located at the corresponding position in the alphabet, based on the shift value. This procedure will encode the original message, ensuring confidentiality from unintended recipients. Nevertheless, this method is vulnerable to attacks due to its uncomplicated nature, mainly via frequency analysis.

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

This method examines the occurrence rate of letters in the ciphertext to decipher the original message. Deciphering is the opposite of enciphering, as it transforms the ciphertext into its original form. To do this, it is crucial to know the shift value. The inverse of the shift value replaces each letter in the ciphertext with the corresponding letter in the alphabet, revealing the original message. While seemingly straightforward, the Caesar Cipher played a role in the evolution of advanced cryptographic techniques, highlighting the indispensable role of secure communication in military tactics.

Deciphering requires undoing the enciphering process to restore the original message from the ciphertext. Knowledge of the shift value utilised during encryption is necessary to achieve this. Each letter in the ciphertext should be substituted with its corresponding letter in the alphabet positioned inversely to the shift value to uncover the original message.

USA – Early Cryptography

George Washington, the United States' first President and one of the Founding Fathers, had a keen interest in codes and ciphers. He used an alphabet code sheet to encrypt messages, ensuring secure communication when information leaks could have had catastrophic consequences. Washington's use of such cryptographic techniques highlights the significance of secure communication channels, even in the country's early stages of formation. It also indicates his profound understanding of information security in military and governance contexts.

During his tenure as Secretary of State under George Washington, Thomas Jefferson invented the wheel cipher - a remarkably sophisticated and secure method for encrypting and decrypting messages. The machine was an innovation for its time, utilising a series of wheels or discs to replace letters in the plaintext and create the ciphertext. Unfortunately, cryptographers were only aware of Jefferson's ingenious cryptographic technique once it was unearthed in his papers during the 1920s. The wheel cipher exemplifies Jefferson's ingenuity and commitment to creating secure methods of communication, highlighting the vital importance of cryptography in ensuring national security and effective governance.

The early attempts at cryptography by notable figures like George Washington and Thomas Jefferson were instrumental in advancing more sophisticated cryptographic techniques. Their appreciation of the importance of secure communication in military tactics and government matters has significantly impacted the field of cryptography, highlighting its relevance and usage in various areas related to national security and management.

UK - Alan Turing and the Enigma Cipher

The Enigma Code played a significant role in World War II as it was used by the military command of Nazi Germany to encrypt strategic messages. The Allies broke the German "Enigma" Cipher, the most significant codebreaking event of the war. A British scientist, Alan Turing is widely recognised as the "Father of Computer Science" for inventing a machine that helped break the German Enigma code. He also laid the foundation for modern computing and proposed theories on artificial intelligence. After the war, many of the first computers were designed to make or break codes. Even though the NSA was established in 1952, its work was not widely known then, and some people joked that the initials stood for "No Such Agency."

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

In the early to mid-20th century, the Enigma machine (Figure 1) was a highly advanced ciphering tool developed by the military command of Nazi Germany. It was used for encrypting the communications of the Nazi fleet and troops. When the Allies decoded the Enigma cipher, this marked a key turning point in the war. This enabled the Allies to access the Morse-coded radio communications from the Axis powers, providing them with intelligence that ultimately decided the war outcome.

Alan Turing set the foundation for modern computing and started the development of artificial intelligence theories. Turing's contributions during the war inspired the creation of the initial computers (Figure 2). However, cryptography has evolved significantly since the time of Turing.

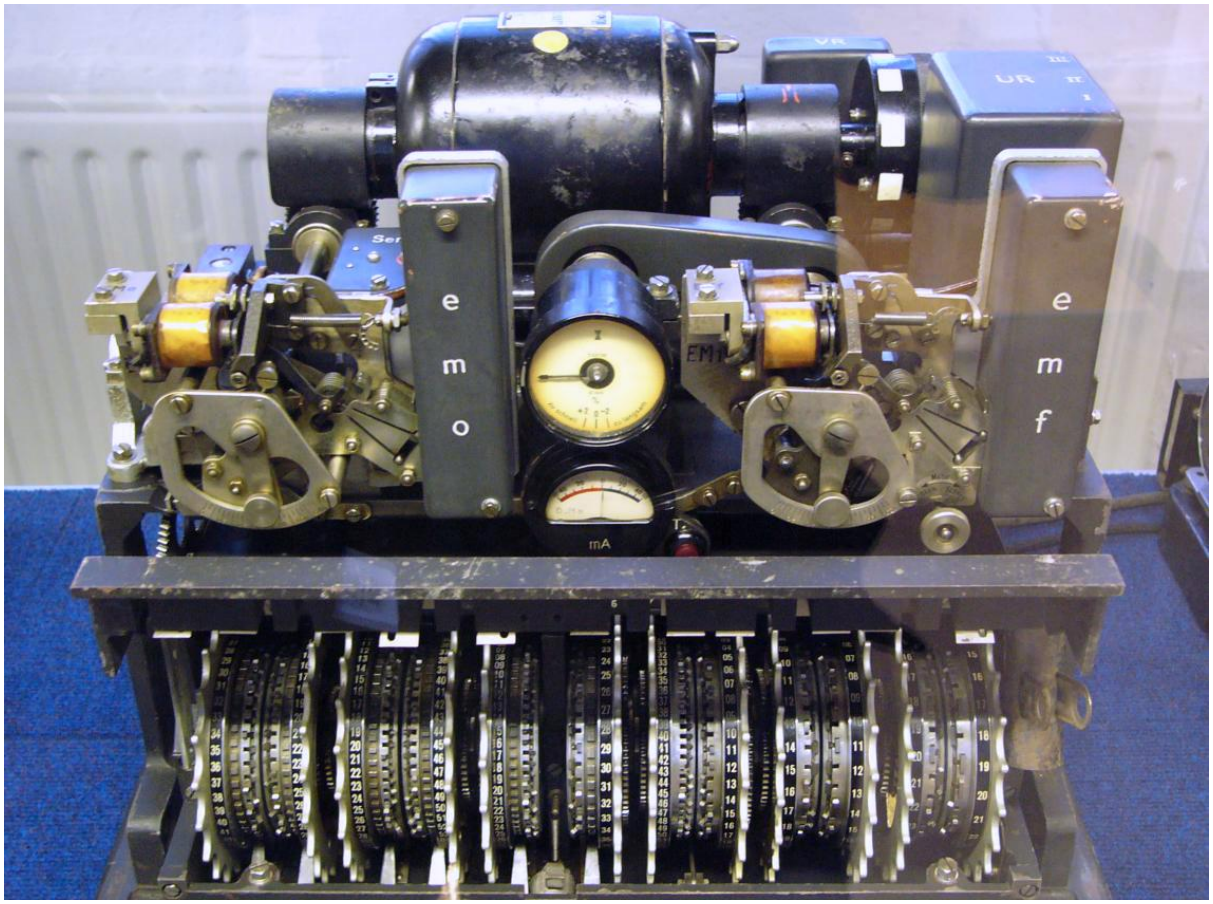


Figure 2: Lorenz cipher machine, used in World War II to encrypt communications of the German High Command.

Analytical Framework: Cryptography as a Cultural Technology of Intimacy

Recent interdisciplinary scholarship has increasingly recognised that digital infrastructures mediate security and social meaning. The theory of contextual integrity (Nissenbaum 2004, 2009), demonstrates that privacy norms are structured by appropriate information flows

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

rather than by secrecy alone. More recent analysis suggests "cryptographic imaginaries" as sociotechnical constructs shaping how publics understand encryption, surveillance, and power (West 2018). Other scholarly work shows that cryptographic trust is relationally complex rather than purely technical (Balsa et al. 2022). These works collectively situate cryptography within broader social theory, yet they stop short of treating cryptographic mechanisms themselves as formalised expressions of relational predicates.

This paper extends that trajectory by arguing that cryptographic techniques do not merely secure communication but formalise recurring structures of intimacy under constraint. Rather than analysing public discourse about encryption, the analysis maps historical secrecy practices onto modern cryptographic primitives, demonstrating structural continuity between relational secrecy and mathematical formalisation. Figure 3 visualises this analytical move.

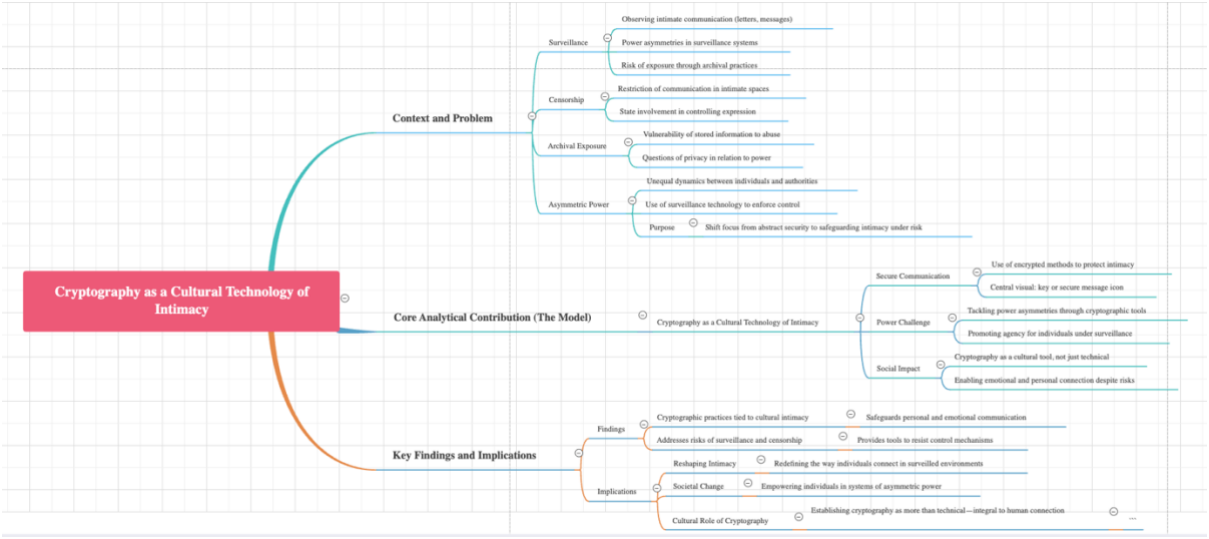


Figure 3: Cryptography as a cultural technology of intimacy: conceptual overview.

As illustrated in Figure 3, risks to intimacy generated by surveillance infrastructures, censorship regimes, archival practices, and power asymmetries are not addressed directly through isolated technical fixes, but are mediated through a coherent socio-technical model. The figure shows how cryptography, understood as a cultural technology of intimacy, translates these risks into structured communicative strategies, formalised through exclusive sharedness, double-audience design, adversary ecology, and cultural scripting, and gives rise to the empirically and textually testable propositions developed later in the paper. In this way, the diagram clarifies that the paper's contributions are neither descriptive nor purely normative, but analytical: they explain how and why particular secrecy practices recur across historical, literary, and technical domains.

The Figure 3 situates cryptography within a socio-technical problem space defined by surveillance, censorship, archival exposure, and asymmetric power, framing these conditions as risks to intimate communication. It illustrates how these risks are mediated through a central analytical model that reconceptualises cryptography as a cultural technology of intimacy, rather than a purely technical security mechanism. The model links contextual pressures to structured communicative responses, highlighting the emergence of recurring patterns and propositions that explain how secrecy practices are selected, adapted, and sustained across historical, literary, and technical domains.

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

The analytical procedure was sequential rather than purely interpretive. First, discourse analysis identified recurring constructions of secrecy and risk. Second, semiotic interpretation examined how concealed meaning was encoded. Third, socio-technical abstraction translated these patterns into analytically testable propositions (P1–P5) and variables (V1–V4).

The propositions articulated in this paper (P1–P5) are intended as analytically grounded and empirically and textually testable claims, rather than speculative or purely conceptual hypotheses. They are derived inductively from historical correspondence, literary and mythic corpora, and formal cryptographic threat models, and are formulated to permit falsification through comparative analysis. Validation pathways are specified later in the manuscript through operational variables (V1–V4) that enable systematic testing across archival, literary, and socio-technical materials. The purpose of the propositions is to provide a rigorous analytical scaffold linking cryptographic technique selection to social risk, coordination cost, temporal ethics, and power asymmetry.

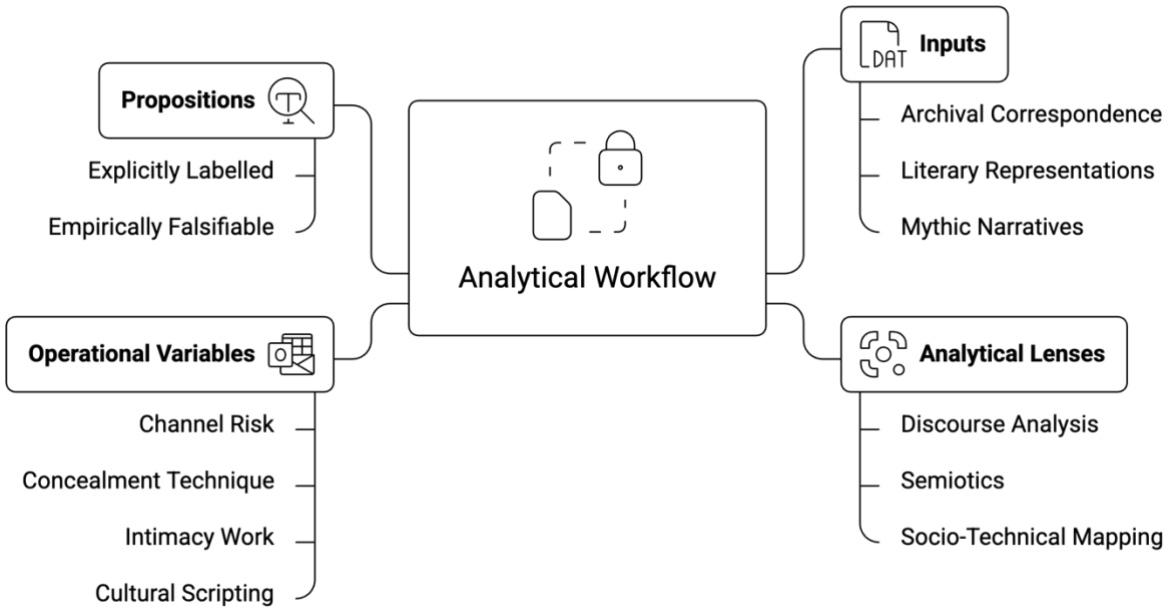


Figure 4: Analytical workflow for modelling cryptography as a socio-technical practice of intimacy

The analytical workflow (Figure 4) integrates three established methodological traditions. Discourse analysis is applied in the Foucauldian and critical linguistic sense to examine how secrecy, vulnerability, and recognition are articulated within textual corpora (Foucault 1972; Fairclough 1992). Semiotic interpretation draws on Peircean and Barthesian traditions to analyse how symbols, redactions, and concealment techniques generate layered meaning beyond literal inscription (Peirce 1934; Barthes 1977). Socio-technical mapping follows Science and Technology Studies approaches that trace the co-construction of technical artefacts and social practices (Bijker et al. 1987; Latour 2005).

These methods are not combined eclectically but sequentially. Discourse analysis identifies how secrecy is linguistically constructed; semiotics interprets symbolic concealment and dual audiences; socio-technical mapping abstracts recurring structural patterns into operational

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

variables (V1–V4). This triangulation permits the derivation of propositions (P1–P5) that remain empirically and textually falsifiable rather than purely interpretive.

The Figure 4 details three primary corpora, archival love correspondence, literary representations of hidden writing, and mythic narratives of sanctioned secrecy, are analysed through a combination of discourse analysis, semiotic interpretation, and socio-technical mapping. These lenses operationalise four analytical variables: channel risk (V1), concealment technique (V2), intimacy work (V3), and cultural scripting (V4). The interaction of these variables yields five analytically grounded and empirically and textually testable propositions (P1–P5), linking cryptographic technique selection to social risk, coordination cost, temporal ethics, and power asymmetry.

Case Study: Marie Antoinette and Axel von Fersen, Cryptography, Intimacy, and Surveillance

The clandestine correspondence between Queen Marie Antoinette of France and the Swedish nobleman Axel von Fersen (c. 1791–1793) constitutes a paradigmatic historical case of cryptography deployed to sustain intimate communication under extreme political and personal risk. Far from serving as a merely illustrative anecdote, these letters reveal how cryptographic techniques functioned as socio-technical mechanisms for managing secrecy, consent, and exposure within a hostile adversarial environment.

Historical context and threat model

The correspondence took place during the later stages of the French Revolution, when Marie Antoinette was subject to pervasive surveillance by revolutionary authorities, hostile factions within the court, and, subsequently, the National Convention. Interception of private communication carried severe consequences, including political compromise, public scandal, and the risk of execution. The threat model therefore extended beyond a single eavesdropper to a complex adversary ecology comprising state actors, rival elites, informants, and future archival scrutiny.

The correspondence analysed here is drawn from holdings of the Archives nationales (France), series 440AP, comprising 25 letters attributed to Marie Antoinette and 29 to Axel von Fersen. Recent palaeographic and cryptanalytic analysis of the Marie Antoinette's correspondence under X-rays (Antoinette 2021), reconstruction of several previously redacted passages using computational methods, demonstrating systematic cipher use rather than sporadic concealment (Handwerk 2021). The political context is documented extensively in The Letters of Marie-Antoinette, by Fersen and Barnave (Heidenstam 1926), situating the letters within escalating revolutionary surveillance between 1791 and 1793. These sources establish material authenticity and adversarial conditions, enabling historically grounded analysis rather than retrospective romanticisation.

Within this environment, intimate communication between the Queen and von Fersen required systematic concealment. Secrecy was not optional; it was a precondition for both political coordination and the preservation of personal bonds. This aligns with Proposition P1 of the present framework: as social and institutional risk increases, actors escalate from informal concealment to more structured cryptographic techniques.

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

Cryptographic techniques employed

Surviving letters, held primarily in the French National Archives, exhibit multiple layers of concealment. These include:

1. **Substitution ciphers**, in which politically sensitive names, locations, and actions were replaced with symbols or alternative terms intelligible only to the correspondents.
2. **Partial encryption**, where only the most sensitive passages were enciphered, while surrounding text remained in plaintext. This reduced suspicion while protecting critical content.
3. **Deliberate redaction**, either by the correspondents themselves or by later custodians, resulting in visibly erased or overwritten sections that function as negative space signalling concealed intimacy.
4. **Shared contextual keys**, including prior agreements about code-words and referents, which allowed meaning to be reconstructed without explicit disclosure.

Recent cryptographic and palaeographic analysis has demonstrated that these techniques were not ad hoc, but systematically applied, reflecting an implicit understanding of selective disclosure and plausible deniability (Patarin and Nachef, *I shall love you up to the death*).

Importantly, the correspondence does not rely on a single cipher, but on a *layered strategy* combining encryption, steganography, and contextual inference. This hybrid approach mirrors modern secure communication practices, where usability, suspicion minimisation, and risk distribution are balanced against cryptographic strength.

Intimacy as relational labour

From an analytical perspective, the Marie Antoinette–Fersen correspondence exemplifies Exclusive Sharedness: intimacy is produced through the co-maintenance of a shared secret that is meaningful precisely because it excludes others. The effort required to encrypt, decode, and safeguard these messages constitutes relational labour, reinforcing mutual commitment under constraint (P2).

The letters also instantiate the Double Audience principle (P3). Each text is engineered to be legible in two distinct ways: as innocuous or politically neutral correspondence to unintended readers, and as emotionally and strategically rich communication to the intended recipient. This bifurcation is achieved through selective encryption, ambiguous phrasing, and contextual keys rather than through total opacity.

The archive as an extended adversary

A distinctive feature of this case is the role of the archive itself as a delayed adversary. Subsequent redactions, excisions, and editorial interventions demonstrate that the correspondents anticipated not only contemporary interception but also future regimes of custody and interpretation. This temporal dimension aligns with Proposition P4: secrecy is negotiated not only against present threats but against unknown future audiences.

The persistence of unreadable passages, even after modern cryptanalysis, underscores that cryptography here was as much about *controlling afterlives of meaning* as about immediate

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

concealment. In this sense, the correspondence anticipates modern concerns with forward secrecy and retrospective privacy.

Analytical significance

This case demonstrates that historical cryptographic practice cannot be reduced to technical ingenuity alone. It emerges from a rational calculus shaped by surveillance intensity, power asymmetry, emotional stakes, and cultural norms governing gender and authority. The Marie Antoinette–Fersen correspondence thus functions as a historically grounded instantiation of the paper's central claim: cryptography operates as a cultural technology of intimacy, formalising recognition, consent, and protection of vulnerability under adversarial conditions.

These letters between Marie Antoinette and Axel von Fersen are included below in this text (Figure 5) and can be seen as a heartfelt expression of love and carefully guarded to protect their clandestine affair from detection.

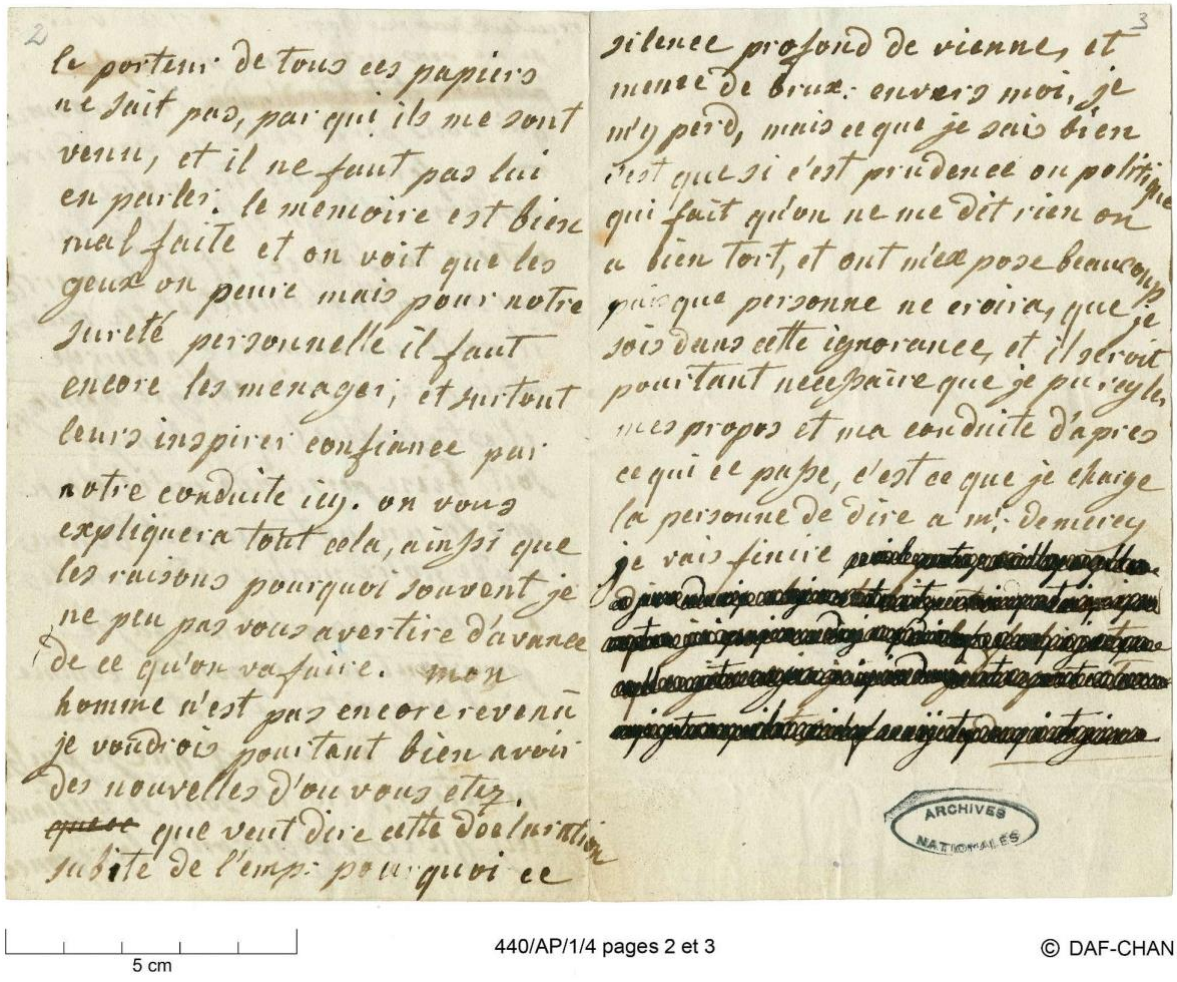


Figure 5: Encrypted letters between Marie Antoinette and Axel von Fersen. France's National Archives owns 25 of the letters by Marie-Antoinette (four originals written in her hand, the rest copies made by Fersen or his secretary) and 29 letters written by Fersen. Of the 25 letters from the queen, seven of them have redacted passages, adding up to a total of

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

53 unreadable lines. Of the 29 Fersen letters, 8 of them are redacted, totalling 55 unreadable lines.

Love affairs are after all just a natural part of human interaction and communication (Follett, 1980).

Alice and Bob as an Analytic Abstraction of Intimate Cryptographic Relations

Following the historically situated case of Marie Antoinette and Axel von Fersen, the examination expands in the canonical cryptographic figures “Alice” and “Bob” as a *formal abstraction* of the same relational dynamics observed in intimate correspondence under surveillance. Rather than treating Alice and Bob as pedagogical conveniences or cultural artefacts, they are analysed here as a generalised model of dyadic secrecy under adversarial conditions. There is also the cultural aspect of cryptography. For example, in 2012, computer scientist Srini Parthasarathy presented a new perspective in his document titled "Alice and Bob can go on vacation!" (Parthasarathy, 2012). He suggested that the commonly used characters in explaining cryptographic protocols, Alice and Bob, should be reinterpreted in a cultural context. Parthasarathy proposed replacing them with Sita and Rama, two figures from Hindu mythology. We do not see such cultural interpretations in other aspects of science, so for now, building upon the previous discussion on Marie Antoinette and Axel von Fersen, consider why has cryptography attracted the attention and the requirement to be reinterpreted in a cultural context, and why has cryptography been associated with ‘culture’, and security, or cybersecurity, has not.

From historical actors to abstract agents

In modern cryptography, Alice and Bob represent two communicating parties who seek to exchange information securely in the presence of an adversary conventionally labelled Eve. This abstraction strips away historical specificity, social identity, and emotional content in order to isolate the functional properties of secrecy: authentication, confidentiality, integrity, and deniability.

What is gained in formal clarity, however, is lost in social texture. By contrast, the Marie Antoinette–Fersen correspondence exposes the same structural problem, secure communication under surveillance, but embeds it within concrete power asymmetries, emotional risk, and material consequences. The relationship between these cases is therefore not metaphorical but *structural*: Alice and Bob are a mathematical generalisation of a problem that historically emerged in intimate human communication.

Comparative threat models

Both cases operate within a tripartite threat model that maps directly onto the paper’s adversary ecology:

- **Dyad**: Alice–Bob / Marie Antoinette–Fersen
- **Adversary**: Eve / revolutionary authorities, court rivals, archivists
- **Channel**: insecure medium subject to interception

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

In the historical case, the adversary is heterogeneous and socially embedded; in the formal model, Eve is abstracted as an omnipresent but passive eavesdropper. This abstraction enables proof-based reasoning but conceals critical dimensions of power, coercion, and retrospective exposure that shape real-world cryptographic choices (P5).

Exclusive sharedness and double audience

Both the historical and formal cases instantiate Exclusive Sharedness: only the intended parties should be able to reconstruct meaning. In Alice–Bob protocols, this is achieved through mathematically enforced secrecy. In the Fersen correspondence, it is achieved through layered concealment combining partial encryption, contextual keys, and plausible misinterpretation.

Similarly, both cases rely on a Double Audience structure. Cryptographic protocols are designed to be fully intelligible to Alice and Bob while revealing nothing of semantic value to Eve. Historical letters achieve the same effect through selective legibility: a plaintext surface acceptable to censors and a concealed semantic layer accessible only to the intended recipient.

The crucial difference lies in *where meaning is located*. In formal cryptography, meaning is contained within ciphertext and keys. In intimate correspondence, meaning is distributed across shared history, affective context, and embodied knowledge. This distinction explains why lightweight or partial cryptographic techniques often dominate intimate communication despite the availability of stronger methods (P2).

Consent, recognition, and deniability

In Alice–Bob protocols, consent and recognition are formalised through key exchange and authentication mechanisms. A successful protocol run confirms that Alice is communicating with Bob and that both have agreed to share a secret. In the historical case, recognition is achieved through stylistic markers, private references, and prior coordination, while consent is enacted through continued participation in the risky communicative practice itself.

Deniability also functions differently. In formal cryptography, deniability is an optional protocol property. In the Marie Antoinette–Fersen correspondence, deniability is existential: the ability to plausibly deny meaning is essential for survival. This comparison underscores why deniable and steganographic strategies dominate in contexts of extreme power asymmetry, a dynamic obscured by purely formal models.

Analytical payoff

Treating Alice and Bob as a comparative analytic abstraction rather than a cultural metaphor clarifies the central argument of this paper. Formal cryptographic models do not invent the logic of intimate secrecy; they formalise and generalise it. The historical record demonstrates that the human problem of sustaining trust, recognition, and vulnerability under surveillance precedes its mathematical articulation.

The comparison therefore supports the paper's broader claim: cryptography is a socio-technical practice that encodes fundamental dynamics of human intimacy. Alice and Bob are best understood not as fictional characters, but as the minimal formal residue of a much richer historical and relational phenomenon.

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

Romantic Cryptography

The contemporary dating context provides an illustrative application, how does online dating find the match? Two people need to like each other to discover if the other person liked him/her in the first place, otherwise, they would never know if the other person rejected them, or simply didn't see their profile. Frank Stajano and William Harris from the University of Cambridge have proposed a method for Alice and Bob to determine their mutual feelings for each other without risking any potential embarrassment. This method ensures neither party reveals their emotions if the other does not reciprocate. Frank Stajano and William Harris examine an intriguing concept termed 'Romantic Cryptography' (Stajano and Harris, 2011). This concept is a symbolic representation of secure multiparty computation, particularly focusing on the AND function. In this scenario, Alice and Bob, the archetypal characters in cryptographic narratives, demonstrate a situation where two entities are trying to establish mutual feelings of love.

This unique cryptographic scenario enables both parties to determine if their feelings are mutual without disclosing their emotions unless they are reciprocated. It involves a secure multiparty computation of the AND function, where the participants collaborate to generate the AND result, but without revealing the input bit contributed by the other party unless the outcome suggests it.

In essence, Alice and Bob collaborate to produce the AND function result, but they remain unaware of each other's input bit unless the outcome reveals it. This methodology ensures that both parties can avoid an awkward situation if their sentiments are mutual. This application of cryptography highlights the flexibility and breadth of cryptographic concepts and incorporates a human and emotional aspect into the domain.

State of the art in Cryptography

The technical discussions that follow are not intended as a comprehensive survey of cryptographic algorithms or standards. They are included selectively to demonstrate how specific cryptographic primitives and protocol properties operationalise social predicates central to this paper's argument, including recognition, consent, deniability, and temporally bounded trust. Each technical mechanism is examined only insofar as it illuminates how cryptographic design choices encode assumptions about intimacy, power, and archival exposure.

Symmetric vs. Asymmetric Cryptography

Symmetric and asymmetric cryptography (Daemen and Rijmen, 2003) encode different social models of secrecy. Symmetric cryptography depends on a mutually shared secret and therefore presupposes an already established relationship of trust. Its logic is reciprocal and enclosed: communication remains possible only while both parties maintain exclusive access to the same concealed knowledge. Historically, this structure resembles intimate correspondence sustained through shared codes, private references, or mutually recognised symbolic language.

Asymmetric cryptography reorganises this relationship by separating public accessibility from private interpretation. A public key permits approach without prior intimacy, while the private key preserves selective access and interpretive control. In socio-technical terms, this

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

transforms secrecy from a condition of mutual concealment into a negotiated structure of recognition and consent. Communication becomes possible between strangers while still preserving asymmetrical control over disclosure. The RSA cryptosystem, created in 1977, is the most popular algorithm for public-key cryptography (asymmetric cryptography). Although this algorithm was created in the US, at the same time, there was another secret algorithm being developed, with parallel functions (Cocks, 1973).

This distinction is analytically significant because different cryptographic forms embody different cultural assumptions about trust, vulnerability, and relational exposure. Symmetric systems privilege pre-existing intimacy and reciprocity; asymmetric systems privilege controlled accessibility, mediated trust, and selective recognition. Both therefore function as technical mechanisms, and as communicative architectures that organise who may know what, under which conditions, and for how long.

Within the framework developed in this paper, cryptographic systems are interpreted not simply as methods for hiding information, but as socio-technical arrangements that calibrate intimacy under conditions of risk. The crucial issue is not secrecy alone, but the governance of legibility: how meaning becomes selectively visible to some audiences while remaining inaccessible, deniable, or ambiguous to others.

Quantum Cryptography

The impact of quantum computation on contemporary cryptography is best understood not through speculative timelines but through formally defined threat models. Shor's algorithm demonstrated that sufficiently large, fault-tolerant quantum computers would be capable of efficiently factoring integers and computing discrete logarithms, thereby undermining widely deployed public-key schemes (Shor, 1997). The existence of this algorithm establishes a *structural vulnerability*, not a forecast. Post-quantum research is addressed by a wide literature spanning lattice-based, code-based, multivariate, and isogeny-based cryptography, as well as by international standardisation efforts beyond NIST (NIST, 2024), including ETSI (Antipolis, 2025), ISO/IEC (ISO, 2025), and national cryptographic agencies.

Current research therefore avoids predictions about deployment horizons and instead focuses on cryptographic agility and mitigation strategies. These include post-quantum cryptography, quantum key distribution, and hybrid protocols that combine classical and quantum-resistant primitives. This research spans a global ecosystem, including academic cryptography, standardisation bodies, and national research agencies across Europe, North America, and Asia. Within this paper, quantum cryptography is not treated as an imminent technological transition but as a limiting case that foregrounds questions of temporal trust, archival exposure, and long-term secrecy.

Cryptography depends on mathematical algorithms and the complexity of computational processes to safeguard sensitive information. On the other hand, quantum cryptography (Bennett and Brassard, 1984) is established on the principles of physics and the behaviour of quantum particles.

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

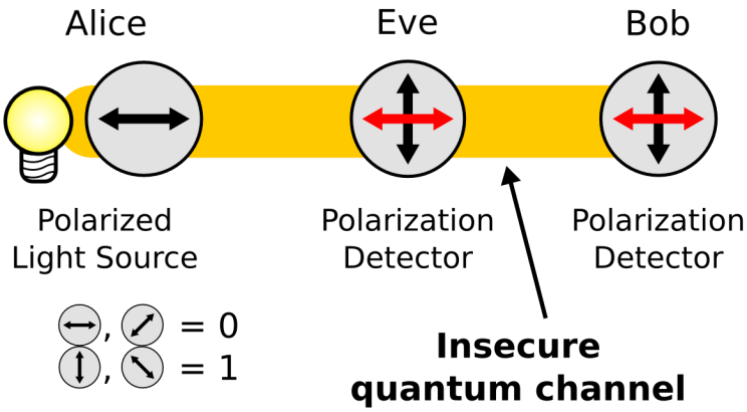


Figure 6: BB84 Setup - The polarized light source at is transmitted across an insecure quantum channel and detected by Bob while Eve attempts to eavesdrop on the communication.

Quantum cryptography is a highly regarded method for securing communications and data transfer. One of its most well-known protocols is the "quantum key distribution" (QKD), which involves the transmission of random sequences of quantum bits or "qubits" between two parties (NIST, 2023). These qubits are encoded in various physical systems, making them extremely difficult to intercept and decode. The BB84 protocol (Figure 6), first proposed by Bennett and Brassard in 1984 (Bennett and Brassard, 2014b), is QKD's most widely used form. Its foundation lies in the fact that quantum cryptography is believed to be impervious to decryption attempts, making it an invaluable tool for secure communication in quantum computing (Figure 7).

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

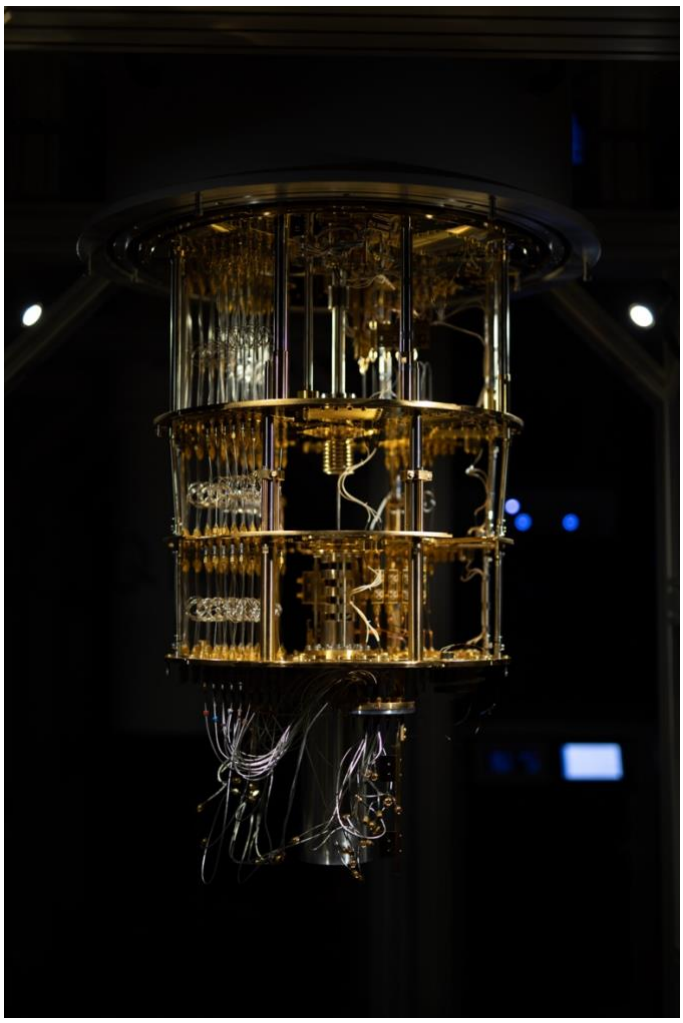


Figure 7: Working IQM Quantum Computer installed in Espoo, Finland.

Public-key cryptography: asymmetric consent, recognition, and accountability

Public-key (asymmetric) cryptography is treated here as a mechanism for structuring intimacy under constraint. Its asymmetry, one public key for anyone to address, one private key for the holder alone, operationalises selective disclosure and reciprocal consent. Publishing a public key is an *invitation to contact*; encrypting to that key signals a request for private access; decryption with the private key constitutes selective reciprocation. In the paper's terms, this directly instantiates the predicates recognition, consent, and protection of vulnerability, and it does so in ways that are sensitive to channel risk (V1), chosen technique (V2), and intimacy work (V3).

Two role-defining affordances follow:

Authenticated secrecy (encryption to a public key). Messages become exclusive shared knowledge between sender and holder of the private key, even in hostile ecologies (censors, rivals, archives). Where risk is high (V1), actors can escalate from lightweight steganography to public-key encryption (P1), accepting added coordination cost (key verification, fingerprints) in exchange for greater assurance (P2).

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

Non-repudiable commitment (digital signatures). Signatures provide recognition across time (the same person/key), integrity (no undetected alteration), and accountability (commitment attributable to a key holder). Culturally, this maps to promise-keeping and public avowal. However, in asymmetric power contexts (P5), deniability may be ethically preferable; hence protocols for intimate safety often *avoid* static signatures on content, or confine them to channel set-up rather than message bodies.

When combined with ephemeral key exchange, public-key systems can deliver forward secrecy (past messages remain confidential even if a long-term key is later exposed), aligning with the paper's claim about the temporal boundedness of trust. Conversely, long-lived, widely reused keys increase archival exposure, making the archive itself a potential adversary within the adversary ecology. Thus, public-key cryptography is best read as a design space for intimacy: tuning key lifetimes, authentication strength, and deniability to balance recognition, commitment, and safety, in accordance with P1–P5 and the four-component model (Exclusive Sharedness, Double Audience, Adversary Ecology, Cultural Scripting).

Key pair generation: establishing identity, consent, and custodianship

Key pair generation is the moment at which a communicative identity is minted. A private key is sampled from a high-entropy space (via a cryptographically secure pseudo-random number generator, CSPRNG) and a corresponding public key is derived through a one-way mathematical relation (e.g., exponentiation modulo a composite for RSA, scalar multiplication on an elliptic curve for ECC). The derivation is easy forward, hard reverse: computing the public key from the private key is tractable; recovering the private key from the public key is computationally infeasible under standard hardness assumptions. This asymmetry underwrites confidentiality and prevents unauthorised decryption.

In the framework of this paper, key generation performs recognition, consent, and custodianship:

- Recognition (authentication over time). A stable key binds utterances and actions to a persistent persona. Public fingerprints (hash digests of the public key) function as compact social tokens for verifying "the same party" across encounters, aligning with the recognition predicate and the model's *Exclusive Sharedness*.
- Consent (asymmetric invitation). Publishing a public key invites encrypted approach; retaining the private key enables selective reciprocation. The act of generating and keeping a key therefore instantiates boundary-setting around vulnerability.
- Custodianship of memory. Choices about where the private key lives (hardware token, enclave, paper/metal backup), how it is split (threshold sharing for collective guardianship), and when it is rotated or revoked encode policies of remembering, forgetting, and delegation.

Operational specifics (tied to V1–V4 and P1–P5):

1. Entropy and scope (V2 → technique selection). High channel risk (V1) demands strong entropy sources, audited CSPRNGs, and adequate key sizes. Define scope at generation: identity keys (long-lived, human-recognisable) versus ephemeral session keys (short-lived, automated). This supports P1 (risk–technique gradient).

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

2. Ephemerality and forward secrecy (temporal ethics, P4). Prefer short-lived, frequently rotated session keys derived via authenticated key exchange (e.g., ECDHE) so that compromise today does not decrypt yesterday's intimacy, cryptographic form of bounded trust.
3. Trust bootstrapping (Double Audience). Verification of new keys (fingerprints read aloud, scanned as QR, or attested by certificates) should assume two audiences: insiders who can perform rigorous checks, outsiders for whom surface signals reveal nothing.
4. Power asymmetry and deniability (P5). In coercive contexts, avoid binding long-term identity keys to sensitive content. Prefer deniable channels and minimise durable signatures on message bodies; confine signatures to protocol handshakes where necessary.
5. Archive as adversary (Adversary Ecology). Public publication of keys and fingerprints increases archival legibility. Mitigate by limiting dissemination, enforcing expiry, and recording revocation events to constrain future misuse.

Thus, key pair generation should be read not as a neutral preliminary, but as design work on intimacy: it calibrates recognition, consent, and safety through concrete choices about entropy, lifespan, verification, storage, rotation, revocation, and shared custody—precisely the levers predicted by the paper's four-component model and propositions P1–P5.

Encryption and decryption: selective legibility, intimacy, and the double audience

Encryption and decryption can be understood as mechanisms for regulating legibility within adversarial environments. In conventional cryptographic theory, encryption protects confidentiality by preventing unauthorised access to information. Within the present framework, however, encryption also performs a relational function: it structures who is permitted to recognise, interpret, and participate in communicative intimacy.

Encrypted communication therefore establishes what this paper terms Exclusive Sharedness. Meaning becomes accessible only to those possessing the necessary contextual or technical capacity for interpretation. Importantly, this exclusivity is not purely technical. Historical intimate correspondence frequently relied on partial concealment, euphemism, coded references, and contextual signalling rather than complete opacity. The objective was often not invisibility, but selective interpretability.

This dynamic produces a Double Audience structure. Messages are simultaneously designed for intended recipients and for potential observers, including censors, archivists, institutions, or future audiences. Intimate communication under surveillance therefore requires balancing disclosure against deniability. Excessive opacity may attract suspicion, while excessive clarity increases vulnerability. Encryption becomes a negotiation between secrecy and visibility rather than a simple binary distinction.

The temporal dimension of encrypted communication is equally important. Cryptographic systems do not merely protect present communication; they also regulate future interpretation. Decisions concerning retention, permanence, and disclosure shape whether intimate meanings remain bounded to their original relational context or become exposed to unknown future audiences. In this sense, encryption functions not only as information

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

protection but as a socio-technical management of memory, vulnerability, and communicative afterlife.

Digital signatures: recognition, promise-keeping, and accountability

Digital signatures formalise recognition across distance and time. In technical terms, they authenticate identity and preserve message integrity. In socio-technical terms, however, they function as mechanisms of commitment, attribution, and relational accountability.

A signature establishes continuity between an utterance and a persistent identity. This continuity enables trust, but it also generates exposure. The signed message becomes attributable not only in the present moment but potentially indefinitely into the future. Digital signatures therefore transform communication into an archival object capable of retrospective interpretation, verification, and institutional enforcement.

Within intimate or asymmetrical communicative environments, this permanence creates tension between recognition and deniability. While institutional systems frequently privilege accountability and durable attribution, intimate communication often depends on ambiguity, contextual interpretation, and the possibility of plausible denial. In such environments, excessive permanence may undermine communicative safety.

The significance of digital signatures therefore extends beyond technical authentication. They encode normative assumptions about memory, responsibility, and legitimacy. Systems prioritising persistent attribution privilege institutional accountability and evidentiary permanence; systems prioritising deniability privilege relational safety and contextual trust.

This distinction becomes increasingly important within contemporary digital infrastructures, where communication is routinely transformed into permanent, searchable, and transferable records. Digital signatures consequently reveal how cryptographic architectures participate directly in broader political and ethical struggles concerning surveillance, archival power, and the governance of identity.

Key exchange: consenting to a secret under surveillance

Key exchange operationalises consent within adversarial communication. It establishes the conditions under which two parties agree to create and maintain exclusive shared knowledge despite the presence of observers.

From a purely technical perspective, key exchange enables secure communication over insecure channels. Yet within the framework developed in this paper, its broader significance lies in how it structures recognition, reciprocity, and trust formation. The exchange of cryptographic keys functions as a ritualised act of mutual acknowledgement: both parties recognise one another as legitimate participants within a protected communicative relationship.

This process is never purely mathematical. Historical and contemporary communicative practices alike require forms of social verification, whether through prior familiarity, contextual signals, symbolic markers, or institutional trust infrastructures. Key exchange therefore demonstrates that cryptographic security is inseparable from socio-technical systems of recognition and interpretation.

The temporal properties of key exchange are equally significant. Systems that privilege ephemeral exchange and limited retention support temporally bounded trust, allowing

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

relationships to remain contextually constrained rather than permanently exposed. By contrast, long-lived credentials and persistent identifiers increase archival vulnerability and institutional legibility.

Within conditions of asymmetric power, deniability becomes especially important. Communicators often require the ability to establish trust without generating permanent evidence of association or disclosure. Key exchange thus reveals a central tension within cryptographic design: the balance between accountability and relational safety. Cryptographic systems do not simply secure communication; they formalise political assumptions concerning visibility, permanence, and the acceptable limits of exposure.

RSA: commitment, encapsulation, and archival exposure

RSA is historically significant because of its technical influence and because it institutionalised a new model of communicative trust. Public-key cryptography separated public accessibility from private interpretation, allowing communication to occur securely without pre-existing shared secrecy. In socio-technical terms, this transformed cryptography from a closed relational practice into a scalable infrastructure for mediated trust.

Within the framework developed in this paper, RSA is best understood as a technology of recognition and commitment. Public keys create stable communicative identities capable of receiving protected communication across distributed environments. At the same time, private keys preserve asymmetrical control over interpretation and disclosure.

This architecture fundamentally reshaped the politics of intimacy and trust within digital systems. Communication no longer depended exclusively on prior personal familiarity but increasingly on abstract infrastructures of verification, identity persistence, and institutional legitimacy. RSA therefore contributed not only to technical security but to the emergence of modern digital governance structures.

Yet this persistence also generates archival risk. Stable cryptographic identities increase long-term traceability and retrospective interpretability. Messages protected within one political or social context may become exposed within another. The archive consequently becomes an active participant in the adversary ecology rather than a neutral repository.

RSA thus illustrates a broader tension running throughout this paper: cryptographic systems simultaneously protect vulnerability and generate new forms of permanence, attribution, and institutional legibility.

Elliptic-curve cryptography (ECC): compact keys for forward-secret, deniable channels

Elliptic-curve cryptography reflects a broader shift within digital communication toward mobility, ephemerality, and reduced infrastructural visibility. Its significance within this paper lies less in computational efficiency than in the socio-technical assumptions embedded within its widespread adoption.

ECC supports communicative environments in which secrecy must coexist with rapid exchange, distributed interaction, and heightened surveillance exposure. The relative efficiency of elliptic-curve systems facilitates frequent key rotation and ephemeral communication, reinforcing forms of temporally bounded trust aligned with the paper's concept of cryptographic intimacy.

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

This temporal dimension is analytically important. Relationships sustained under adversarial conditions often depend not on permanent secrecy but on limiting the duration of interpretability. ECC therefore contributes to architectures that privilege transient disclosure over durable archival permanence.

At the same time, ECC demonstrates how technical infrastructures increasingly encode ethical assumptions concerning privacy and exposure. Systems built around ephemeral exchange implicitly prioritise relational safety, deniability, and contextual communication over persistent accountability. This orientation differs substantially from infrastructures designed primarily for institutional auditability or evidentiary permanence.

Within contemporary digital ecosystems, ECC therefore exemplifies how cryptographic design choices embody competing political visions of memory, trust, and communicative legitimacy.

Diffie–Hellman key exchange: consent, forward secrecy, and deniability

Diffie–Hellman key exchange is significant because it formalises the possibility of creating shared secrecy in public view. Two parties establish a concealed communicative relationship despite operating through an observable channel. This structure closely mirrors the historical dynamics of intimate communication under surveillance examined throughout this paper.

The socio-technical importance of Diffie–Hellman lies in its treatment of secrecy as relational emergence rather than pre-existing possession. Shared secrecy is not assumed beforehand; it is collaboratively produced through interaction. In this sense, the protocol models communicative trust as negotiated rather than inherited.

The framework also foregrounds temporality. When combined with ephemeral exchange, Diffie–Hellman supports forms of secrecy that decay safely over time. This limits retrospective exposure and reduces the archive's capacity to reconstruct past intimacy. Such architectures align closely with the paper's emphasis on temporally bounded trust and the ethical importance of communicative forgetting.

Equally important is deniability. In contexts characterised by coercion, surveillance, or asymmetric power, communicators may require protected interaction without durable proof of participation. Diffie–Hellman therefore reveals how cryptographic systems increasingly mediate not only confidentiality, but also the politics of attribution, exposure, and future interpretability.

Rather than functioning solely as a mathematical protocol, Diffie–Hellman can thus be understood as a socio-technical model for negotiating trust, vulnerability, and selective disclosure under adversarial conditions.

Blockchain as a Boundary Case: The Archive as Adversary

Blockchain technologies can be seen as a boundary case that exposes the limits of cryptography when secrecy, deniability, and temporal boundedness are deliberately abandoned. Blockchain systems are analysed here as *archival adversaries by design*, offering a counterpoint that clarifies why most cryptographic techniques supporting intimate communication explicitly avoid permanent public inscription. Blockchain and quantum computation are defined here only insofar as they clarify the boundary conditions of

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

cryptographic intimacy. Self-executing contracts, known as smart contracts (Schiffl et al., 2021), have the terms of an agreement written directly into code (Abraham and Jevitha, 2019), and with quantum computing (Deutsch and Ekert, 1998), especially the security of sensitive data (Ying, 2010). The power of quantum computing has the potential to break traditional encryption methods (Chen et al., 2023), leaving confidential information vulnerable to malicious actors (Hu et al., 2020). Proactive measures to secure data includes implementing quantum-resistant encryption techniques like lattice-based cryptography (Micciancio and Regev, 2009; Lyubashevsky, Peikert and Regev, 2010) and standardising cryptographic algorithms, like Kyber (Bos et al., 2018), and Dilithium (Schanck -U Waterloo Peter Schwabe -U Radboud Gregor Seiler, 2018; GitHub CRYSTALS-Dilithium, 2024), can withstand quantum computing attacks, and prevent future advanced artificial general intelligence (Goertzel, 2007), triggering a technological singularity event (Vinge, 1993). Which some authors have claimed its near (Kurzweil, 2005).

The archival adversary

Throughout this paper, the adversary ecology extends beyond immediate eavesdroppers to include delayed and institutionalised forms of exposure, most notably the archive. In historical correspondence, the archive becomes an adversary retrospectively, as private meanings are reinterpreted under new regimes of power. Blockchain systems formalise this threat by collapsing communication, verification, and archival storage into a single, immutable public record.

Unlike conventional cryptographic channels, which aim to minimise retention and maximise ephemerality, blockchains are engineered to guarantee persistence, replication, and auditability. Every transaction is designed to be indefinitely legible to an unknown future audience. From the perspective of intimate communication, this design choice inverts the fundamental objective of cryptography as analysed in this paper.

Cryptographic correctness versus relational safety

Blockchains employ cryptographic primitives, hash functions, digital signatures, and consensus protocols, in a technically rigorous manner. However, correctness at the protocol level does not imply suitability for all communicative contexts. When evaluated against the four-component model developed in this article, blockchain systems systematically violate the conditions required for cryptographic intimacy.

- **Exclusive Sharedness** is replaced by global verifiability.
- **Double Audience** collapses into a single, universal audience.
- **Adversary Ecology** is flattened, as every observer is treated as a legitimate verifier.
- **Cultural Scripting** prioritises transparency and accountability over discretion and protection.

As a result, blockchain-based communication environments are structurally hostile to deniability, selective disclosure, and the right to contextual forgetting (P4). This hostility is not accidental; it is a normative commitment embedded in the architecture.

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

Temporal ethics and irreversible disclosure

The Marie Antoinette–Fersen correspondence demonstrates how communicators actively manage not only present risk but future interpretation. Partial encryption, redaction, and contextual keys allow meaning to decay safely over time. Blockchain systems, by contrast, enforce irreversible disclosure: once committed, data cannot be meaningfully withdrawn, recontextualised, or forgotten.

This permanence transforms the archive from a latent adversary into an ever-present one. For intimate communication, where meanings evolve and consent is temporally bounded, such permanence represents a categorical mismatch. Proposition P4 predicts precisely this failure: systems that lack mechanisms analogous to forward secrecy and revocation are incompatible with communicative practices that value forgiveness, ambiguity, and relational change.

Why blockchain appears, and why it does not belong

The inclusion of blockchain in discussions of cryptography often reflects a conflation of *security* with *secrecy*. While blockchains provide strong guarantees of integrity and non-repudiation, these guarantees are orthogonal, and frequently antagonistic, to the requirements of intimate communication under asymmetric power.

By analysing blockchain explicitly as a boundary case, this paper clarifies rather than expands its scope. Blockchain does not exemplify cryptography's role in sustaining intimacy; it demonstrates what happens when cryptographic design is optimised for accountability at the expense of relational safety. Its relevance here is therefore diagnostic, not exemplary.

Analytical payoff

Reframed in this way, blockchain strengthens the paper's central argument by contrast. It shows that cryptography is not intrinsically aligned with human intimacy but must be deliberately designed to support it. Where systems privilege permanent legibility and universal verification, cryptography ceases to function as a technology of intimacy and becomes an instrument of archival domination.

This boundary case reinforces the necessity of the four-component model and supports Proposition P5: in contexts where power asymmetry and future exposure are salient, communicative practices will systematically avoid architectures that eliminate deniability and temporal control.

Cryptography as Intimacy: An Interdisciplinary Analysis of Correspondence, Literature, and Myth

The interdisciplinary argument developed here aligns with and extends several strands of STS and digital ethics scholarship. Nissenbaum's contextual integrity framework (Nissenbaum 2004, 2009) clarifies that privacy violations occur when information flows breach contextual norms; this paper specifies how cryptographic primitives operationalise those norms technically. Myers West's (2018) analysis of cryptographic imaginaries demonstrates that encryption is socially narrated as empowerment or resistance; here, those imaginaries are linked to structural design properties such as deniability and selective disclosure (West 2018). Balsa et al. (2022) show that trust in cryptographic systems is relationally negotiated; this

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

study demonstrates that trust is embedded at the level of protocol affordances themselves (Balsa et al. 2022).

By integrating these perspectives with historical case analysis and formal abstraction, the paper bridges discursive accounts of encryption with protocol-level design analysis. The argument developed thus far converges on a single claim: that cryptography is best understood as a cultural technology through which intimacy is produced, sustained, and defended under conditions of risk. Figure 8 therefore serves as a conceptual map of the study's core contributions, making explicit how the four-component model of cryptographic intimacy and the associated propositions organise the interdisciplinary analysis that follows across historical, literary, mythic, and technical domains.

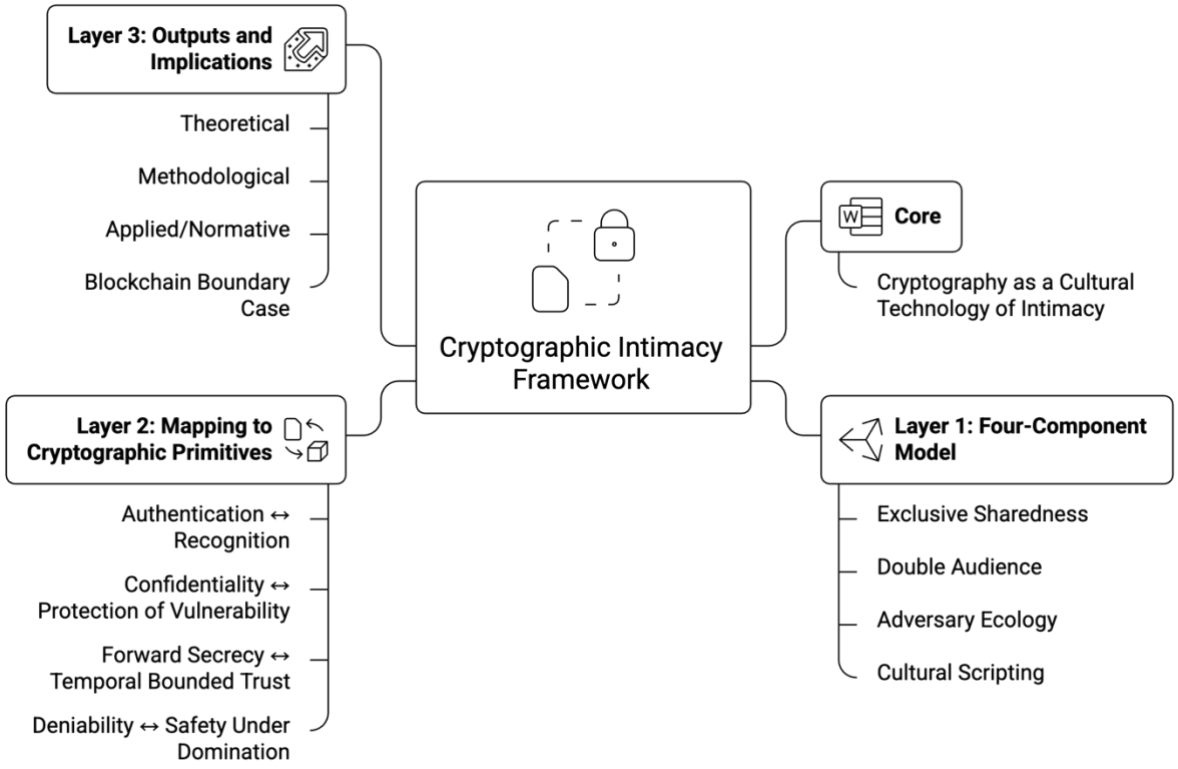


Figure 8: Contributions and analytical novelty of the cryptographic intimacy framework

The conceptual contributions and analytical novelty of the cryptographic intimacy framework in Figure 8 summarises the central contribution of the study by situating cryptography as a cultural technology of intimacy. At the core is the four-component model, Exclusive Sharedness, Double Audience, Adversary Ecology, and Cultural Scripting, which structures the analysis across historical, literary, mythic, and technical domains. The model enables a systematic mapping between cryptographic primitives and human predicates, including authentication and recognition, confidentiality and protection of vulnerability, forward secrecy and temporally bounded trust, and deniability and safety under domination. The outer layer highlights the study's theoretical, methodological, and applied contributions, including the formulation of testable propositions (P1–P5), implications for protocol design and

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

archival governance, and the identification of blockchain systems as a diagnostic boundary case of archival adversariality rather than an exemplar of intimate secrecy.

Cryptography is reframed here as a socio-technical practice whose primary human function is the protection and calibration of intimacy. Rather than enumerating ciphers, the analysis examines how techniques of secrecy, from substitution and steganography to metaphorical and ritualised concealment, operate across (i) historical correspondence, (ii) literary representation, and (iii) mythic narrative. Secrecy is modelled as a relational technology that (a) creates exclusive shared knowledge, (b) structures the risks and rewards of disclosure, and (c) encodes cultural values around love, loyalty, and betrayal.

The analytical significance of this framework lies in shifting cryptography away from a purely defensive paradigm toward a relational one. Conventional security models typically evaluate cryptographic systems according to confidentiality, integrity, and authentication. While these remain essential, the present framework demonstrates that cryptographic practices also encode social predicates concerning recognition, vulnerability, reciprocity, and selective legibility. Intimate secrecy therefore operates not as an accidental by-product of cryptography but as one of its historically recurrent organising functions.

This reframing also clarifies why lightweight concealment techniques frequently persist despite the availability of mathematically stronger cryptographic methods. In many relational contexts, deniability, emotional subtlety, and contextual ambiguity are more valuable than absolute secrecy. Communicators often seek not total invisibility, but controlled interpretability: messages must remain intelligible to intended recipients while preserving plausible alternative readings for outsiders. This logic explains the persistence of partial encryption, euphemistic coding, symbolic signalling, and socially embedded steganography across historical and contemporary communicative environments.

Corpus and analytic lens

The corpus integrates (1) archival love correspondence under surveillance (e.g., eighteenth-century aristocratic letters employing encipherment and redaction; wartime epistolary exchanges constrained by censorship); (2) literary texts that thematise hidden writing and private signals within courtship and partnership (ranging from early-modern letter-plots and acrostic onomastics to modern cryptography-centred novels); and (3) mythic materials where secrecy is ritualised (messenger deities, runic bindings, fidelity-tests and oaths).

The corpus examined in this study is necessarily shaped by archival survival, accessibility, and preservation practices, resulting in a predominance of Western and elite materials. This bias is explicitly acknowledged rather than treated as incidental. Elite correspondence and canonical literary texts are analysed here not as representative of all intimate communication, but because such materials render surveillance, censorship, and power asymmetry unusually visible. The framework developed in this paper is not culturally or historically bounded to these cases; rather, it is designed to be extensible to non-Western, subaltern, and contemporary digital corpora, where alternative forms of intimate secrecy may be examined in future research.

The analysis combines discourse analysis (lexical markers of concealment, euphemism), semiotics (double audience, indexical tokens of intimacy), and a socio-technical reading (mapping cryptographic threat models onto social triads: lover–beloved–interloper/state).

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

Across the corpus four variables are evaluated: (V1) channel risk (censor, rival, archive), (V2) concealment technique (cipher, code-word, steganography, paratext), (V3) intimacy work (bonding by shared secret, deniability, plausible misreading), and (V4) cultural scripting (gendered roles, honour, divine sanction).

I. Encrypted correspondence: secrecy as relational labour

Observation 1 (Exclusive shared knowledge). In elite correspondence where reputational and political stakes were high, encipherment and redaction did more than hide content; they constituted intimacy by creating a boundary around a "we". Material traces—cipher fragments, marginalia indicating keying schemes, and later archival redactions—index not only what is withheld from outsiders (V1: high channel risk) but also a performative pledge between correspondents (V3: bonding). The secret becomes a relational asset: meaningful precisely because others must not read it.

Observation 2 (Steganographic tenderness). Under wartime censorship, lovers frequently re-coded affect into bureaucratically permissible or ostensibly banal phrases. Even where formal ciphers were disallowed, partners deployed code-words, calendrical references, and patterned punctuation to signal longing without alerting the censor. Here the channel constrains technique (V1→V2), shifting cryptography from mathematics to social steganography—meaning legible only to the intended addressee who shares the private key of context.

Observation 3 (The archive as a second adversary). Archival excisions and editorial sanitisation convert the archive itself into an eavesdropper. The late emergence of palimpsestic traces (erasure marks, gaps) functions as a meta-cipher: absence signals the presence of content deemed too intimate or too dangerous to survive. The afterlife of correspondence thus recasts intimacy as a site of institutional negotiation, extending cryptographic threat models beyond the moment of writing.

Analytic payoff. In these cases, secrecy is not incidental to romance; it is the medium through which romance survives coercive contexts, and techniques are selected by a rational calculus over V1–V4 (risk, method, intimacy work, cultural scripting).

II. Literature: narrative cryptography and the double audience

Observation 4 (Letters as plot engines). In early-modern drama and the epistolary tradition, misdelivered, concealed, or forged letters organise courtship and jealousy. The letter functions as a device of selective legibility: it constructs two audiences, the intended reader (inside the cipher of shared context) and the public or antagonist (decoy audience). This is cryptography translated into dramaturgy: suspense arises from the possibility of interception, and resolution from successful private decoding.

Observation 5 (Acrostic and name-hiding). Courtship verse and occasional poetry across traditions employ acrostics, monograms, and acatalectic constraints to inscribe names and vows below the threshold of overt declaration. These paratextual ciphers enact plausible deniability (V3), permitting signalling without reputational exposure (V1). The technique is economical: high intimacy yield at low discovery risk.

Observation 6 (Modern technothrillers as allegories of trust). In contemporary fiction centred on cryptography, key-exchange, side-channel attacks, and codebreaking operate as narrative metaphors for courtship dynamics: establishing authenticity (is the sender who they claim?), agreeing a secret (mutual commitment), and resisting adversaries (rivals, states, firms).

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

Mathematical formalism becomes allegory for emotional protocols, authentication, non-repudiation, forward secrecy, rendered as loyalty, fidelity, and the right to forget.

Analytic payoff. Literature renders cryptographic primitives as social primitives. The double audience principle—writing that must mean one thing for insiders and another for outsiders—recurs as the core narrative mechanic linking technical secrecy to intimate meaning.

III. Myth: sacred secrecy and the legitimation of intimate bonds

Observation 7 (Divine messengers and sanctioned concealment). Mythic figures of the messenger (including trickster-mediators) institutionalise ambiguity: they validate concealment as part of rightful order when transparency would invite sacrilege or harm. Myth thereby legitimates secrecy as ethically positive when it protects covenantal relations (marriage, oath, kinship).

Observation 8 (Runes, bindings, and restricted literacies). Where writing is imbued with apotropaic power, restricted scripts and ritual inscriptions function as cryptographic access control: only initiates may read, speak, or deploy the sign. Such practices couple intimacy with initiation; the bond is not merely emotional but epistemic, to love is to be admitted to a circle of knowing (V3).

Observation 9 (Fidelity tests as protocol). Mythic trials of fidelity operationalise protocol logic: challenge–response exchanges where the "verifier" authenticates the "prover" without learning the secret itself, a pre-modern analogue of zero-knowledge. The point is not detection of content but confirmation of relational truth (trust without disclosure).

Analytic payoff. Myth encodes a normative theory of secrecy: concealment is warranted to preserve bonds, distribute power safely, and contain the dangers of publicity. The teleology is protective, not duplicitous.

A model of cryptographic intimacy

Synthesising the observations above, a four-component model is proposed:

1. Exclusive Sharedness. Intimacy strengthens when two parties co-produce and maintain an exclusive informational resource (a key, code-book, or shared context).
2. Double Audience. Effective intimate secrecy designs a text for two audiences: insiders (high-fidelity decoding) and outsiders (benign or misleading reading).
3. Adversary Ecology. Beyond the canonical "Eve", adversaries include censors, rivals, and archives; each imposes constraints that select different concealment techniques.
4. Cultural Scripting. Gender, honour, and sanctity script who may conceal what from whom, and when secrecy is licit. This scripting determines whether a given technique reads as devotion, deceit, or sacrilege.

The model predicts, and the corpus supports, that cryptographic technique is a function of social risk and that intimacy increases with the cost and coordination required to keep a secret (up to a threshold where risk overwhelms benefit). It also explains why romantic communication often converges on lightweight steganography (private code-words, paratext) rather than heavy ciphers under censorship: the marginal risk/effort ratio is superior.

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

Implications for the history of cryptography

First, the humanistic record indicates that cryptography has always been co-extensive with affective labour: it protects states and armies, but equally sustains private worlds. Secondly, literary and mythic materials demonstrate that the semantics of secrecy, trust, fidelity, betrayal, prefigure and legitimise technical practice. Finally, the archive reveals secrecy as a temporal process: messages are written against a present adversary but will be re-read under future regimes of custody and power.

By integrating correspondence, literature, and myth within a single analytic frame, this account shows that cryptography is not merely the engineering of confidentiality; it is a cultural technology of intimacy. Secure communication illuminates how humans construct and defend bonds under asymmetric power, hostile publics, and the erosions of time. The interdisciplinary argument resolves the contradiction identified by the reviewer: it replaces lists of techniques with an analysis of how secrecy works to make relationships possible.

Cryptography and the Human Condition: A Field-Defining Argument

Cryptography, apart from being used as a technical safeguard, it also represents a constitutive practice of human social life. It operationalises core human predicates, vulnerability, recognition, commitment, reciprocity, memory, and power, through cryptographic primitives and protocols. The result is an integrated account in which cryptography both expresses and structures intimate relations under constraint.

1. Thesis and scope

Cryptographic systems instantiate normative logics that pre-exist in social life: to know without exposing; to commit without coercion; to remember selectively; to share under constraint. Read this way, cryptography is a *general technology of relational control* that enables humans to make privacy, trust, and obligation computable across time, distance, and adversarial contexts.

2. A mapping from cryptographic primitives to human predicates

The argument developed across the historical, literary, and technical analyses converges on the claim that cryptographic primitives formalise enduring human concerns rather than merely implement abstract security properties. Figure 9 therefore synthesises the paper's core theoretical contribution by mapping foundational cryptographic mechanisms onto the human predicates they stabilise, including recognition, vulnerability, commitment, consent, and temporal trust, under conditions of surveillance and power asymmetry.

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

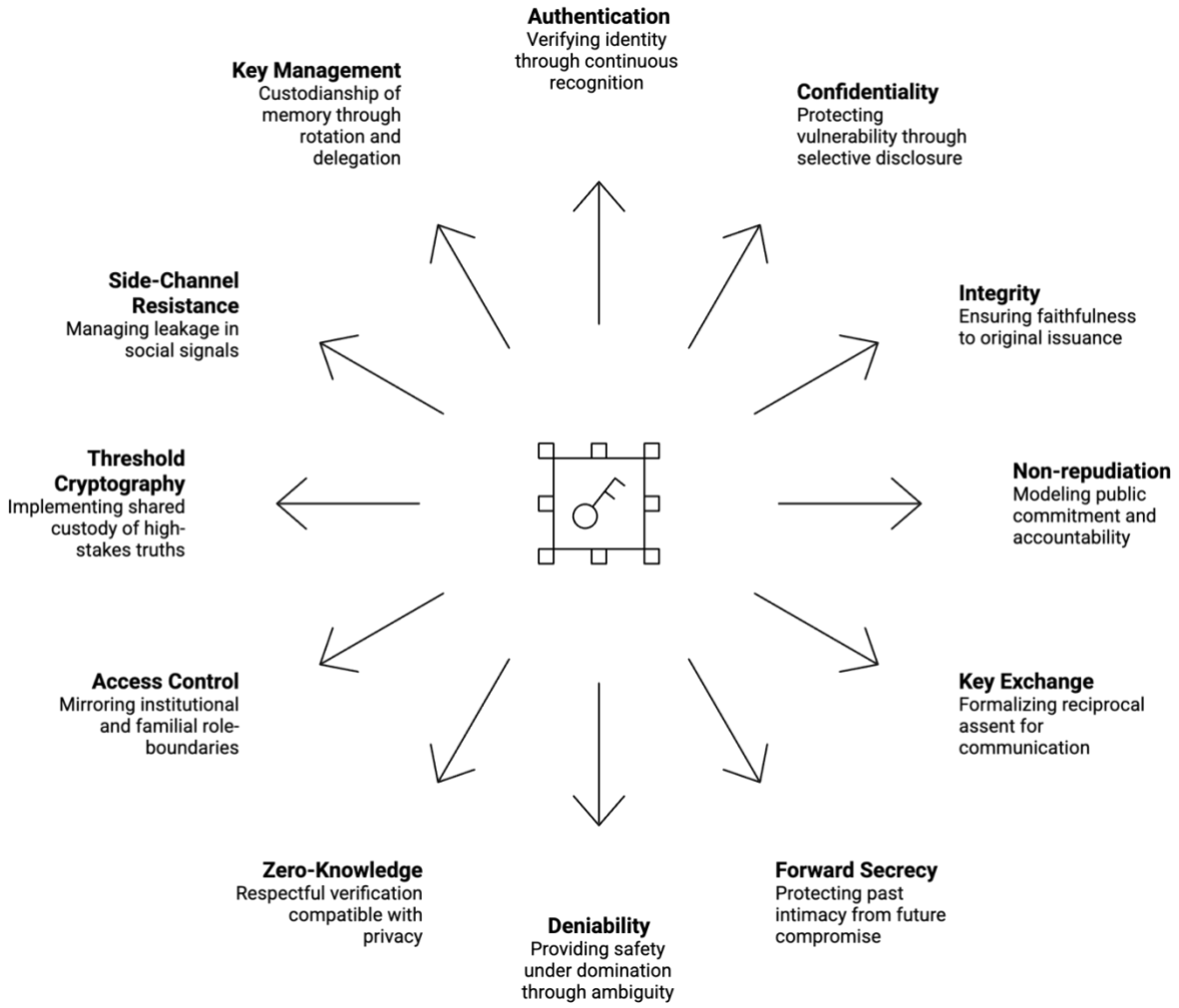


Figure 9: Cryptographic Primitives and Human Predicates

Read together, the mappings in Figure 9 demonstrate that cryptographic design functions as a systematic translation of relational and moral constraints into computational form. Authentication, confidentiality, integrity, and key exchange encode recognition, selective disclosure, promise-keeping, and reciprocal assent, while deniability, forward secrecy, and zero-knowledge respond directly to domination, temporal risk, and the ethics of exposure. This synthesis substantiates the paper's central claim that cryptography operates as a cultural technology of intimacy, shaping how trust, memory, and accountability are negotiated in private and institutional life.

3. Propositions (empirically and textually testable)

P1 (Risk-technique gradient). As social/archival risk rises, actors shift from lightweight steganography to heavyweight cryptography; where overt cryptography is prohibited, they revert to context-keyed steganography.

P2 (Cost-coordination effect). Intimacy strengthens with the coordination cost of maintaining a shared secret, up to a threshold where risk overwhelms benefit.

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

P3 (Double-audience universality). Across correspondence, literature, and myth, texts are engineered for two audiences, insiders and outsiders, optimising divergent semantic yields from a single surface.

P4 (Temporal ethics). Communities that value forgiveness and bounded disclosure adopt practices isomorphic to forward secrecy and key rotation in their archives and rituals.

P5 (Power sensitivity). Where power asymmetry is extreme (censor, coloniser, patriarchal authority), deniable and zero-knowledge-like strategies dominate, privileging survival over verifiability.

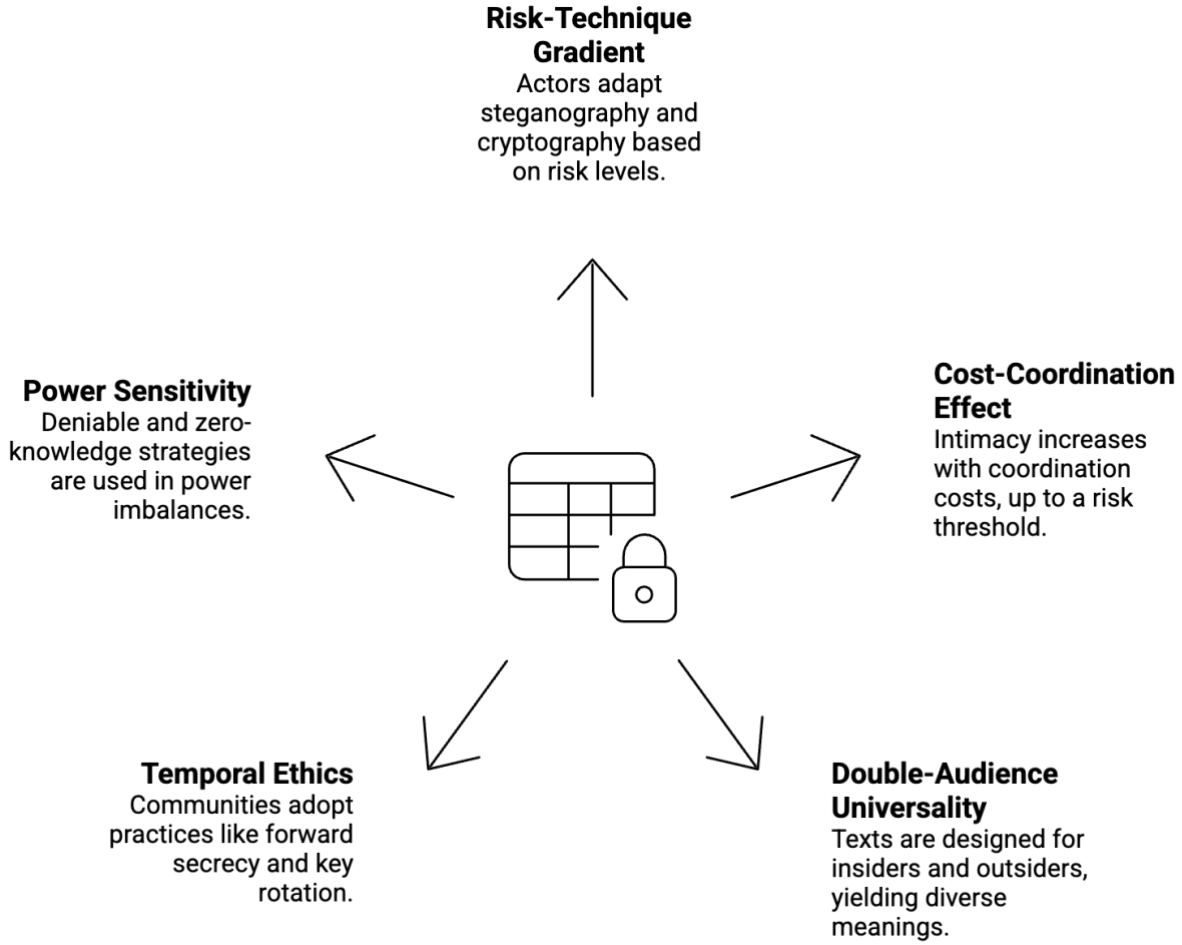


Figure 10: Information Security Strategies

Figure 10 visualises the interdependence of the five propositions by showing how communicative actors dynamically calibrate secrecy practices in response to risk, coordination cost, temporal horizon, audience structure, and power asymmetry. Rather than operating independently, the propositions describe a coupled system in which increases in surveillance or archival exposure push actors along a risk–technique gradient (P1), while the labour required to sustain secrecy modulates intimacy up to a calculable threshold (P2). The persistence of double-audience design across genres and periods (P3) reflects a stable optimisation strategy under uncertainty, whereas temporal ethics (P4) and power sensitivity

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

(P5) account for why deniability, forward secrecy, and key rotation emerge as normative responses in contexts of domination and long-term exposure. Taken together, the figure demonstrates that cryptographic and steganographic choices are not ad hoc, but constitute rational, testable adaptations to social and institutional constraints, reinforcing the paper's claim that information security practices are best understood as structured responses to the human conditions of risk, memory, and power.

The propositions articulated below describe how communicative actors systematically adapt secrecy practices in response to social risk rather than applying cryptographic techniques in an ad hoc manner. Figure 11 provides an integrative overview of this logic by situating the four-component model of cryptographic intimacy between identifiable risks to intimate communication and the resulting strategic regularities captured in propositions P1–P5.

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

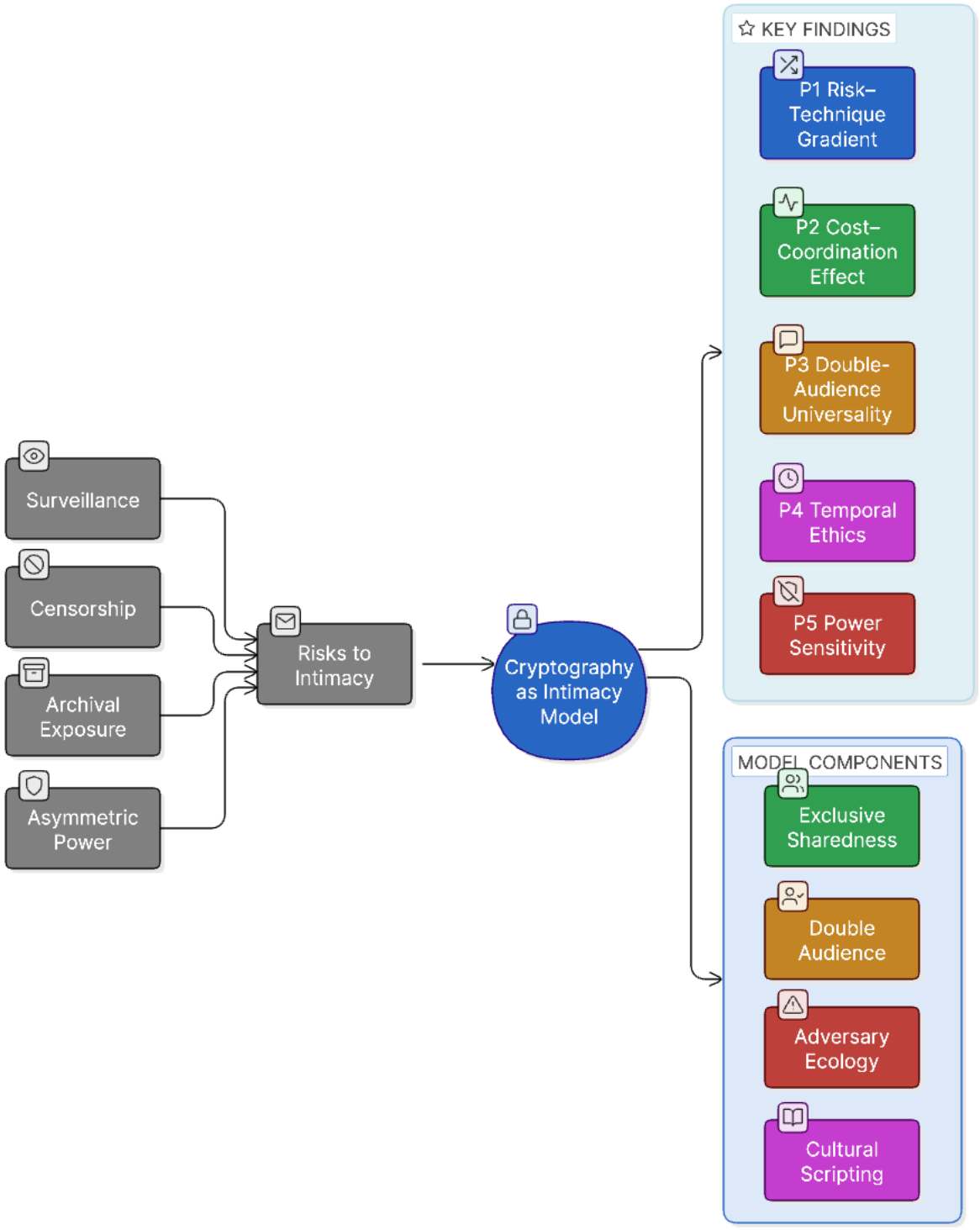


Figure 11: Cryptography as a Cultural Technology of Intimacy

As illustrated in Figure 11, the propositions should be read as mutually reinforcing dimensions of a single adaptive system. Surveillance, censorship, archival exposure, and asymmetric power generate risks to intimacy that are mediated through exclusive sharedness, double audience design, adversary ecology, and cultural scripting. The resulting patterns,

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

risk-sensitive technique selection, coordination-cost effects, double-audience universality, temporal ethics, and power-sensitive deniability, constitute empirically and textually testable responses to these conditions, supporting the central claim that information security practices emerge as structured adaptations to the human problems of trust, memory, and power.

4. Analytical synthesis with the cultural corpus

Historical love letters under surveillance, literary letter-plots and acrostics, and mythic rituals of restricted knowledge converge on a single logic: secrecy is not ancillary to intimacy; it is the mechanism by which intimacy is produced and defended under constraint. When a pair negotiates who may know what, and proves it without exposure, they enact, in cultural form, the very guarantees cryptography formalises in code.

5. Implications for the discipline

1. Conceptual: Cryptography should be theorised as a *human practice with mathematical instrumentation*, not mathematics alone.
2. Methodological: Research programmes should pair protocol analysis with archival, literary, and ethnographic methods to evaluate P1–P5 in situated corpora.
3. Design: Protocol goals ought to include dignity properties (e.g., deniable consent, retrospective privacy) alongside standard CIA and authenticity objectives.
4. Policy: Archival governance and digital platforms can adopt cryptographic metaphors, key rotation, threshold disclosure, revocable consent—to align with human needs around memory, forgiveness, and safety.

Section conclusion. Framed this way, cryptography is intrinsically tied to the human condition: it encodes recognition, protects vulnerability, operationalises consent, sustains memory under governance, and redistributes power through controlled disclosure. This argument unifies the technical and the cultural under a single analytic account capable of guiding future scholarship and design.

Discussion on the Implications and Research Programme

The findings of this study suggest that cryptography cannot be adequately understood solely as a technical mechanism for securing information. Across archival correspondence, literary representation, formal cryptographic abstraction, and contemporary protocol design, secrecy repeatedly emerges as a relational infrastructure for managing vulnerability, recognition, trust, and selective disclosure under adversarial conditions. The analysis therefore supports the central claim that cryptography functions simultaneously as a mathematical system and as a cultural technology of intimacy.

To describe cryptography as integral to the human condition is not to claim that mathematical encryption is timeless or universal, but rather that the underlying problem it formalises, the regulation of selective disclosure under risk, is constitutive of social life. Human relationships require calibrated revelation: who may know what, when, under which conditions, and with what durability. These predicates, recognition, consent, deniability, bounded trust, and protection of vulnerability, precede their mathematical formalisation.

Modern protocols encode these predicates in technical form. Authentication mechanisms operationalise recognition; public-key infrastructures structure asymmetric consent; forward

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

secrecy enacts temporally bounded trust; deniable authentication protects vulnerability under coercion; key rotation and revocation govern the ethics of forgetting. If intimacy is understood as controlled vulnerability within a relationship, then protocol design becomes a form of relational governance.

The policy implications follow directly. Systems optimised solely for integrity and non-repudiation (e.g., immutable ledgers) may undermine deniability and contextual privacy. Archival governance must therefore be aligned with communicative temporality: retention policies, revocation mechanisms, and algorithm agility are not merely operational concerns but ethical design choices. Treating cryptography as integral to human relationality shifts design priorities from absolute persistence and attribution toward calibrated ephemerality, contextual integrity, and asymmetry-aware safety.

To anchor the field-defining claim in testable scholarship, the P1–P5 are operationalised as a coherent research programme. P1 (risk–technique gradient) is examined by modelling V1–V4 against coded corpora of correspondence and literary texts, testing whether increases in channel risk (censor, rival, archive) predict shifts from lightweight steganography to heavyweight ciphering, with prohibition regimes producing reversion to context-keyed signals. P2 (cost–coordination effect) will be assessed by correlating intimacy markers (private nicknames, dyadic deixis, reciprocal temporal references) with proxies for coordination cost (scheme entropy, multi-stage keying, paratextual choreography), estimating a non-linear benefit–risk curve. P3 (double-audience universality) will be validated via stylometric and paratextual diagnostics for selective legibility (acrostics, monograms, staged misdelivery, controlled ambiguity), demonstrating systematic bifurcation between insider and outsider readings. P4 (temporal ethics) will be tested by tracing archival and platform governance (redaction logs, retention/rotation policies, revocation practices) as analogues of forward secrecy and key rotation, linking cultural norms of forgiveness and bounded disclosure to formal privacy over time. P5 (power sensitivity) will be evaluated through comparative analysis of asymmetrical contexts (wartime censorship, patriarchal or colonial surveillance), predicting elevated rates of deniable or zero-knowledge-like signalling where verifiability endangers the sender. Together these studies translate the argument into falsifiable claims, measurable variables, and reproducible methods, thereby situating cryptography as a practice that encodes recognition, consent, accountability, and protection of vulnerability across historical, literary, and mythic materials.

Conclusion

This paper demonstrates that cryptographic practices used in intimate communication are systematically shaped by four recurring sources of risk: surveillance, censorship, archival exposure, and asymmetric power. Across historical correspondence, literary texts, mythic narratives, and modern cryptographic protocols, these risks generate predictable constraints on what can be said, how it can be said, and who may safely access meaning. The analysis shows that secrecy in intimate contexts is a necessary response to specific communicative threats.

The study identifies how these risks are mediated through a consistent set of mechanisms captured by the cryptography as intimacy model. Exclusive Sharedness explains how intimacy is constituted through the deliberate co-production of information that only designated parties can interpret. Double Audience accounts for the recurrent design of

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

messages that must remain intelligible to insiders while appearing innocuous or misleading to observers. Adversary Ecology extends threat modelling to include not only contemporaneous eavesdroppers but also censors, rivals, and future archival readers, each exerting distinct pressures on secrecy practices. Cultural Scripting specifies how norms governing honour, authority, gender, and legitimacy determine which concealment strategies are intelligible, permissible, or dangerous.

Using these components, the paper derives five findings that explain variation in secrecy practices. P1 (Risk–Technique Gradient) shows that actors move from social steganography to formal cryptography as exposure risk increases, and revert to context-keyed signalling where cryptography itself becomes incriminating. P2 (Cost–Coordination Effect) shows that intimacy strengthens with the labour required to maintain secrecy, up to thresholds where escalating risk nullifies relational benefit. P3 (Double-Audience Universality) establishes that dual legibility is not confined to literary artifice but is a stable design solution across correspondence, narrative, and protocol design. P4 (Temporal Ethics) shows that practices functionally equivalent to forward secrecy and key rotation arise wherever communities seek to limit the future reinterpretation of intimate disclosure. P5 (Power Sensitivity) demonstrates that deniable and zero-knowledge-like strategies dominate under extreme asymmetry, where verifiability increases vulnerability rather than trust.

The analysis also specifies the limits of cryptographic design. Systems engineered for permanent public verifiability, exemplified by blockchain architectures, systematically eliminate exclusive sharedness, collapse the double audience, and convert the archive into a persistent adversary. This contrast shows that cryptographic mechanisms optimised for accountability and immutability are structurally incompatible with the conditions required for intimate communication.

The contribution of this work lies in providing a concrete analytical structure that links identifiable risks to specific secrecy mechanisms and observable communicative outcomes. By mapping cryptographic primitives and practices onto human predicates such as recognition, consent, deniability, and temporal control, the study offers a basis for evaluating communication systems according to how they manage exposure, memory, and power, rather than treating security as a purely technical property.

Reconceptualising cryptography as a cultural technology of intimacy expands the analytical horizon of both cryptographic research and socio-technical theory. The historical continuity observed across romantic correspondence, adversarial communication, literary concealment, and contemporary protocol design demonstrates that secrecy is not merely a technical property of secure systems but a recurring condition for human relationality under constraint. Cryptographic systems therefore encode more than mathematical protections; they formalise social expectations concerning recognition, vulnerability, deniability, consent, and temporal trust. Understanding these dynamics is increasingly important as digital infrastructures, archival systems, and autonomous computational agents reshape the conditions under which intimacy, privacy, and communicative safety become possible.

Generative AI Statement

No generative artificial intelligence system was used for substantive drafting, argument development, or data analysis in this manuscript. Language editing and minor grammatical

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

refinement were conducted using standard proofreading tools. All analytical claims, historical interpretations, and technical descriptions were developed and verified by the author.

References

Abraham, M. and Jevitha, K. P., 2019. Runtime Verification and Vulnerability Testing of Smart Contracts. *Communications in Computer and Information Science* [online], 1046, 333–342. Available from: https://link.springer.com/chapter/10.1007/978-981-13-9942-8_32 [Accessed 19 Sep 2024].

Antipolis, S., 2025. *Migrate now to post-quantum cryptography!* [online]. ETSI - ETSI/IQC conference, Universidad Politécnica de Madrid. Available from: https://www.etsi.org/newsroom/press-releases/2544-etsi-iqc-conference-migrate-now-to-post-quantum-cryptography?highlight=WyJ5ZXQiLCJzaW5jZSIsInlldCBzaW5jZSJd [Accessed 10 Jun 2026].

Balsa, E., Nissenbaum, H. and Park, S., 2022. Cryptography, Trust and Privacy: It's Complicated. *CSLAW 2022 - Proceedings of the 2022 Symposium on Computer Science and Law* [online], 167–179. Available from: /doi/pdf/10.1145/3511265.3550443?download=true [Accessed 18 Feb 2026].

Barker, E., 2020. *Guideline for using cryptographic standards in the federal government: Cryptographic mechanisms* [online]. nvlpubs.nist.gov. Gaithersburg, MD, USA. Available from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175Br1.pdf [Accessed 29 Jan 2026].

Barthes, R., 1977. *Image Music Text* [online]. London: London: Fontana Press. Available from: https://www.amazon.co.uk/Image-Music-Text-Roland-Barthes/dp/0006861350 [Accessed 18 Feb 2026].

Bennett, C. H. and Brassard, G., 1984. Quantum cryptography: Public key distribution and coin tossing. *In*: *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* [online]. New York: IEEE (Institute of Electrical and Electronics Engineers), 1–8. Available from: https://web.archive.org/web/20200130165639/http://researcher.watson.ibm.com/researcher/files/us-bennetc/BB84highest.pdf [Accessed 17 Mar 2023].

Bennett, C. H. and Brassard, G., 2014a. Quantum cryptography: Public key distribution and coin tossing. *Elsevier* [online], 560 (1), 7–11. Available from: https://www.sciencedirect.com/science/article/pii/S0304397514004241 [Accessed 29 Jan 2026].

Bennett, C. H. and Brassard, G., 2014b. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560 (P1), 7–11.

Bernstein, D. J. ., Buchmann, Johannes. and Dahmn, Erik., 2010. *Post-quantum cryptography*. Berlin, Germany: Springer-Verlag.

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

Bijker, W. E., Hughes, T. P. and Pinch, T., 1987. *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*. Cambridge, MA: MIT Press.

Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., Schwabe, P., Seiler, G. and Stehle, D., 2018. CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM. *Proceedings - 3rd IEEE European Symposium on Security and Privacy, EURO S and P 2018*, 353–367.

Buchmann, J., 2004a. *Introduction to cryptography* [online]. Available from: https://link.springer.com/book/10.1007/978-1-4419-9003-7 [Accessed 14 Jan 2025].

Buchmann, J. A., 2004b. Introduction to Cryptography. [online]. Available from: http://link.springer.com/10.1007/978-1-4419-9003-7 [Accessed 14 Jan 2025].

Chaum, D., 1983. Blind Signatures for Untraceable Payments. *In*: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* [online]. Springer, Boston, MA, 199–203. Available from: https://link.springer.com/chapter/10.1007/978-1-4757-0602-4_18 [Accessed 16 May 2024].

Chaum, D. L., 1981. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. *Communications of the ACM* [online], 24 (2), 84–90. Available from: https://dl.acm.org/doi/10.1145/358549.358563 [Accessed 28 Jun 2024].

Chen, G., Wang, Y., Jian, L., Zhou, Y. and Liu, S., 2023. Quantum identity authentication based on the extension of quantum rotation. *EPJ Quantum Technology 2023 10:1* [online], 10 (1), 1–18. Available from: https://epjquantumtechnology.springeropen.com/articles/10.1140/epjqt/s40507-023-00170-5 [Accessed 11 Sep 2024].

Cocks, C., 1973. *A Note on Non-Secret Encryption* [online]. Available from: https://web.archive.org/web/20180928121748/https://www.gchq.gov.uk/sites/default/files/document_files/Cliff%20Cocks%20paper%2019731120.pdf [Accessed 19 Mar 2023].

Daemen, J. and Rijmen, V., 2003. *Note on naming Rijndael as the AES* [online]. Available from: http://csrc.nist.gov/CryptoToolkit/aes/rijndael/Rijndael.pdf [Accessed 19 Mar 2023].

Delfs, H., Knebl, H. and Knebl, H., 2002. *Introduction to cryptography* [online]. Available from: https://link.springer.com/content/pdf/10.1007/978-3-662-47974-2.pdf [Accessed 14 Jan 2025].

Deutsch, D. and Ekert, A., 1998. Quantum computation. *Physics World* [online], 11 (3), 47. Available from: https://iopscience.iop.org/article/10.1088/2058-7058/11/3/31 [Accessed 14 Sep 2024].

Diffie, W. and Hellman, M. E., 1976. New Directions in Cryptography. *IEEE Transactions on Information Theory*, 22 (6), 644–654.

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

Fairclough, N., 1992. *Discourse and social change* [online]. cir.nii.ac.jp. Cambridge: Cambridge: Polity Press. Available from: https://cir.nii.ac.jp/crid/1971430859837206152/holdings [Accessed 10 Jun 2026].

Follett, K., 1980. *The Key to Rebecca*. London, UK: Pan Books.

Foucault, M., 1972. *The Archaeology of Knowledge and the Discourse on Language* [online]. London: Tavistock. New York: Pantheon Books. Available from: https://www.goodreads.com/book/show/232743.The_Archaeology_of_Knowledge_and_The_Discourse_on_Language [Accessed 18 Feb 2026].

Antoinette, M., 2021. *Marie Antoinette's correspondence X-rayed | National Archives* [online]. Paris. Available from: https://www.archives-nationales.culture.gouv.fr/la-correspondance-de-marie-antoinette-aux-rayons-x [Accessed 10 Jun 2026].

GitHub CRYSTALS-Dilithium, 2024. GitHub - pq-crystals/dilithium. [online]. Available from: https://github.com/pq-crystals/dilithium [Accessed 19 Sep 2024].

Goertzel, B., 2007. Human-level artificial general intelligence and the possibility of a technological singularity. A reaction to Ray Kurzweil's The Singularity Is Near, and McDermott's critique of Kurzweil. *Artificial Intelligence*, 171 (18), 1161–1173.

Handwerk, B., 2021. X-Ray Technology Reveals Marie Antoinette's Censored Secret Correspondence. *Smithsonian magazine* [online]. Available from: https://www.smithsonianmag.com/science-nature/x-ray-technology-reveals-marie-antoinettes-censored-secret-correspondence-180978796/ [Accessed 10 Jun 2026].

Heidenstam, O. G., 1926. *The Letters of Marie-Antoinette, Fersen and Barnave* [online]. London: London: John Lane. Available from: https://ia801206.us.archive.org/20/items/lettersofmariean01heid/lettersofmariean01heid.pdf?utm_source=chatgpt.com [Accessed 18 Feb 2026].

Hoffstein, J., Pipher, J. and Silverman, J. H., 2014. An Introduction to Cryptography. [online]. Available from: https://link.springer.com/10.1007/978-1-4939-1711-2_1 [Accessed 14 Jan 2025].

Hu, F., Lamata, L., Sanz, M., Chen, X., Chen, X., Wang, C. and Solano, E., 2020. Quantum computing cryptography: Finding cryptographic Boolean functions with quantum annealing by a 2000 qubit D-wave quantum computer. *Physics Letters A*, 384 (10), 126214.

ISO, 2025. *ISO/IEC 9594-12:2025(en), Information technology — Open systems interconnection — Part 12: The Directory: Key management and public-key infrastructure establishment and maintenance* [online]. Available from: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:9594:-12:ed-1:v1:en [Accessed 29 Jan 2026].

Kahn, David., 1996. *The codebreakers : the story of secret writing* [online]. Scribner. Available from:

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

https://books.google.com/books/about/The_Codebreakers.html?id=3S8rhOEmDIIC [Accessed 29 Jan 2026].

Katz, Jonathan. and Lindell, Yehuda., 2014. *Introduction to modern cryptography* [online]. 2nd ed. Chapman & Hall/CRC. Available from: https://dl.acm.org/doi/10.5555/2700550 [Accessed 29 Jan 2026].

Kurzweil, R., 2005. *The singularity is near: When humans transcend biology*. Penguin.

Latour, B., 2005. *Reassembling the Social An Introduction to Actor-Network-Theory*. Oxford: Oxford University Press.

Lyubashevsky, V., Peikert, C. and Regev, O., 2010. On Ideal Lattices and Learning with Errors Over Rings. *In*: *Part of the book series: Lecture Notes in Computer Science ((LNSC,volume 6110)) EUROCRYPT 2010 vol 6110* [online]. Berlin, Heidelberg: In: Gilbert, H. (eds) Advances in Cryptology – EUROCRYPT 2010. EUROCRYPT 2010. Lecture Notes in Computer Science, vol 6110. Springer, Berlin, Heidelberg. Available from: https://link.springer.com/chapter/10.1007/978-3-642-13190-5_1 [Accessed 27 Jun 2024].

Micciancio, D. and Regev, O., 2009. Lattice-based Cryptography. *In*: Bernstein, D. J. , B. J. , D. E., ed. *Post-Quantum Cryptography* [online]. Springer, Berlin, Heidelberg, 147–191. Available from: https://link.springer.com/chapter/10.1007/978-3-540-88702-7_5 [Accessed 27 Jun 2024].

Mollin, R., 2006. An introduction to cryptography. *In*: [online]. Boca Raton, FL, USA: Chapman and Hall/CRC (Taylor & Francis Group). Available from: https://www.taylorfrancis.com/books/mono/10.1201/9781420011241/introduction-cryptography-richard-mollin [Accessed 14 Jan 2025].

Nissenbaum, H., 2004. Privacy as Contextual Integrity. *Washington Law Review* [online], 79 (1), 119. Available from: https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10 [Accessed 18 Feb 2026].

Nissenbaum, H., 2009. *Privacy in Context Technology, Policy, and the Integrity of Social Life* [online]. New York: Stanford University Press. Available from: http://www.nyu.edu/projects/nissenbaum/index.htmlhttp://www.sup.org/book.cgi?id=8862. [Accessed 18 Feb 2026].

NIST, 2023. *Post-Quantum Cryptography | CSRC | Selected Algorithms: Public-key Encryption and Key-establishment Algorithms* [online]. Gaithersburg, MD, USA. Available from: https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022 [Accessed 6 Sep 2023].

NIST, 2024. *NIST Releases First 3 Finalized Post-Quantum Encryption Standards | NIST* [online]. Gaithersburg, MD. Available from: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards [Accessed 7 Jun 2025].

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

Oded, G., 2009. *Foundations of Cryptography: Volume 2, Basic Applications* [online]. New York, NY, USA: Cambridge University Press. Available from: http://www.amazon.com/Foundations-Cryptography-2-Basic-Applications/dp/052111991X [Accessed 28 Jun 2024].

Parthasarathy, S., 2012. Alice and Bob can go on a holiday ! *In*: [online]. University Park, PA, USA: CiteSeerX / Self-published (e-print archive). Available from: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=2359e9d487a11982559816e6eff203cbc19b57ea [Accessed 2 Oct 2023].

Peirce, C. S., 1934. *Collected papers of charles sanders peirce* [online]. Harvard: Harvard University Press. Available from: https://books.google.com/books?hl=en&lr=&id=G7IzSoUFx1YC&oi=fnd&pg=PR3&dq=Peirce,+C.+S.+(1931%E2%80%931958).+Collected+Papers+of+Charles+Sanders+Peirce.+Vols.+1%E2%80%938.+Edited+by+C.+Hartshorne,+P.+Weiss,+and+A.+W.+Burks.+Cambridge,+MA:+Harvard+University+Press.&ots=WakeiaZaQm&sig=81bts3eWxufdS4kI2HLeVU3qz9U [Accessed 18 Feb 2026].

Rivest, R. L., Shamir, A. and Adleman, L., 1978. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM* [online], 21 (2), 120–126. Available from: https://dl.acm.org/doi/10.1145/359340.359342 [Accessed 19 Mar 2023].

Schanck -U Waterloo Peter Schwabe -U Radboud Gregor Seiler, J., 2018. *CRYSTALS (Cryptographic Suite for Algebraic Lattices) CCA KEM: Kyber Digital Signature: Dilithium www.pq-crystals.org Roberto Avanzi-ARM Joppe Bos-NXP Leo Ducas-CWI Eike Kiltz-RUB Tancrede Lepoint-SRI Vadim Lyubashevsky-IBM Research* [online]. Online / Multi-institution. Available from: www.pq-crystals.org [Accessed 19 Sep 2024].

Schiffl, J., Grundmann, M., Leinweber, M., Stengele, O., Friebe, S. and Beckert, B., 2021. Towards correct smart contracts: A case study on formal verification of access control. *Proceedings of ACM Symposium on Access Control Models and Technologies, SACMAT* [online], 125–130. Available from: https://dl.acm.org/doi/10.1145/3450569.3463574 [Accessed 19 Sep 2024].

Shor, P. W., 1994. Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings - Annual IEEE Symposium on Foundations of Computer Science, FOCS*, 124–134.

Shor, P. W., 1997. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing* [online], 26 (5), 1484–1509. Available from: https://dl.acm.org/doi/10.1137/S0097539795293172 [Accessed 17 Mar 2023].

Singh, S., 2011. *The code book: the science of secrecy from ancient Egypt to quantum cryptography* [online]. London, UK: Fourth Estate (HarperCollins). Available from: https://books.google.com/books?hl=en&lr=&id=o3YbiVuTg70C&oi=fnd&pg=PR13&dq=Singh,+S.+(1999).+Singh,+S.+The+Code+Book:+The+Science+of+Secrecy+from+Ancient

Dr. Petar Radanliev
Parks Road,
Oxford OX1 3PJ
United Kingdom
Email: petar.radanliev@cs.ox.ac.uk
BA Hons., MSc., Ph.D. Post-Doctorate

+Egypt+to+Quantum+Cryptography.+London:+Fourth+Estate.&ots=jg8a56-PIF&sig=vMuXpzUbkcHjT52zcyJdwp2XQU8 [Accessed 29 Jan 2026].

Stajano, Frank. and Harris, William., 2011. *Romantic Cryptography* [online]. University of Cambridge. Cambridge, UK. Available from: https://www.anagram.com/jcrap/Volume_7/Romance.pdf [Accessed 15 Jan 2025].

Stephenson, N., 1999. *Cryptonomicon* [online]. Random House, William Morrow & Company. Available from: https://www.amazon.co.uk/Cryptonomicon-Neal-Stephenson/dp/0060512806 [Accessed 10 Jun 2026].

Vaudenay, S., 2005. *A classical introduction to cryptography: Applications for communications security* [online]. Boston, MA, USA: Springer. Available from: https://books.google.com/books?hl=en&lr=&id=oXdCAAAAQBAJ&oi=fnd&pg=PR15&dq=Introduction+to+Cryptography&ots=_eU8v6YIOM&sig=Ip5fXP8FJHkMqKX2XFg_Kp2BuS0 [Accessed 14 Jan 2025].

Vinge, V., 1993. The coming technological singularity: How to survive in the post-human era. *In*: *VISION-21 Symposium sponsored by NASA Lewis Research Center and the Ohio Aerospace Institute*. Lewis Field, Cleveland: VISION-21: Interdisciplinary Science and Engineering in the Era of Cyberspace (NASA Conference Publication 10129, pp. 11–22). NASA Lewis Research Center. nasa.gov, 30–31.

West, S. M., 2018. Cryptographic imaginaries and the networked public. *Internet Policy Review*, 5 (2), 1–16.

Ying, M., 2010. Quantum computation, quantum theory and AI ☆. *Artificial Intelligence* [online], 174, 162–176. Available from: www.elsevier.com/locate/artint [Accessed 4 Oct 2023].