The Encryption Dilemma: Balancing Secure Communication and Lawful Access through Multi-Stakeholder Responsibility

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree Bachelor of Science in Computer Science, School of Engineering

Jonghyun Lee

Spring 2025

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

MC Forelle, Department of Engineering and Society

Introduction

Data are often referred to as the oil of the 21st century (Stach, 2023). The importance of data has continuously increased, reflecting its growing valuation as a strategic asset across both the private and public sectors (Fleckenstein et al., 2023). As a result, the methods for securing and encrypting data have naturally evolved in response to this heightened importance. The global encryption software market is expected to reach USD 60.7 billion by 2033 (Pangarkar, 2025). This significant growth underscores the escalating demand for encryption solutions driven by the need to secure data against increasingly sophisticated cyber threats. Encryption serves as a cornerstone for privacy protection and cybersecurity, enabling secure communications, protecting sensitive data, and underpinning trust in digital services.

However, encryption's protective qualities also create significant complications for law enforcement and national security agencies. Criminal actors exploit encrypted platforms to evade detection, presenting profound challenges for investigations. This duality raises the critical policy question: how can societies maintain the security benefits of strong encryption while ensuring criminal investigations can proceed effectively?

This paper explores this tension by analyzing the technical aspects of encryption technologies, legal frameworks, and policy alternatives. While it focuses primarily on developments in the United States, it also incorporates comparative insights from other major jurisdictions, including Australia and India, to examine how different legal and political systems approach encryption policy. This paper argues that balanced encryption policies can only be achieved through collaborative efforts among stakeholders, combining strong security with practical support for law enforcement.

Literature Review

Current debates surrounding encryption policy often involve complex intersections among technological requirements for data security, legal demands for investigative transparency, and moral considerations regarding privacy and public safety. Numerous studies underscore how robust encryption methods significantly enhance user privacy but simultaneously hinder the investigative capabilities of law enforcement agencies.

A study on Dutch criminal cases illustrates that law enforcement utilizes significantly more technical investigations often in cases involving highly secure encrypted platforms such as End-to-End Encryption (E2EE) — a cryptographic method that ensures only the communicating users can access message contents, thereby excluding even service providers and law enforcement from accessing the data (IBM, 2021), placing additional burdens on investigative authorities and ultimately on the taxpayer (Hartel & van Wegberg, 2023). The challenges faced by law enforcement are clearly reflected in statistics, as the FBI disclosed that encryption prevented access to evidence in 650 of 5,000 devices examined between 2015 and 2016, and in 1,200 of 2,800 devices between October and December 2016. This suggests that the difficulty of investigating criminal activities increases significantly as encryption technologies continue to evolve (Manpearl, 2017).

Legislative responses attempting to address these challenges have led to complex debates. In the United States, multiple legislative efforts—most notably the EARN IT Act, first introduced in 2020 and reintroduced in 2022 and 2023—sought to impose accountability on platforms for user-shared content, potentially discouraging the implementation of encryption due

to increased liabilities (EARN IT Act of 2020, S.3398, 116th Congress; EARN IT Act of 2022, S.3538, 117th Congress; EARN IT Act of 2023, S.1207, 118th Congress). However, critics argue that such measures undermine overall internet security and compromise user privacy rights by indirectly pressuring companies to weaken encryption standards to avoid legal repercussions (Abelson et al., 2015). Similarly, Australia enacted the Telecommunications and Other Legislation Amendment (TOLA) Act in December 2018, empowering law enforcement to compel technology providers to assist in accessing encrypted data. Despite its intentions, the act has received substantial criticism due to concerns about weakened cybersecurity and significant economic impacts on tech companies (Barker et al., 2021).

Some researchers advocate a systemic approach that simultaneously respects privacy rights and meets national security requirements. In 2018, lawful hacking was proposed as an alternative that does not require weakening encryption itself but instead leverages existing vulnerabilities or targeted techniques to assist investigations (Bellovin et al., 2018). Despite extensive research, a notable gap remains in effectively balancing user privacy with lawful investigative access through practical and secure technical solutions.

This paper employs STS framework to analyze encryption policy, emphasizing the interplay between technological infrastructure, regulatory frameworks, societal demands, and ethical considerations. STS theory facilitates understanding how encryption technologies and policies can be co-constructed to manage tensions between privacy and lawful access effectively. From an STS perspective, concepts such as "going dark"—the phenomenon where law enforcement cannot access digital evidence due to encryption—are analyzed not merely as technical issues but as outcomes of complex socio-technical interactions influenced by technology evolution, policy decisions, and societal privacy norms.

Further research is necessary to explore these innovative cryptographic techniques and their feasibility as realistic policy alternatives. Integrating these approaches into comprehensive encryption policy frameworks could present solutions that reconcile the conflicting needs of privacy, security, and lawful access.

Methods

This paper employs two methods: case study analysis and policy analysis. The case study of Telegram and policy analysis of the U.S. and several other countries. The methodology is designed to provide insights into how encryption technologies hinder law enforcement investigations and how existing policies address these challenges and the current limitations.

Telegram was selected as the primary case study for various reasons. It is currently the fourth most widely used messaging app world-wide. Not only that, both the app and its CEO have recently been involved in legal controversies. Also, Telegram implements end-to-end encryption (E2EE) method in their “secret chats” ensuring that only the intended sender and recipient of a message can access its content, rendering intercepted communications unintelligible to third parties, including law enforcement (IBM, 2021). This case study will help readers grasp the difficulties that the law enforcement agencies are currently facing.

Data for policy analysis were collected from official government publications, legislative records, academic literature, and reports from international organizations such as the United Nations and the European Commission, to capture a comprehensive range of perspectives. The policies analyzed include the U.S. EARN IT Act (introduced initially in 2020, then reintroduced in 2022 and 2023), Australia's Telecommunications and Other Legislation Amendment (TOLA)

Act (passed in December 2018), the U.S. Clarifying Lawful Overseas Use of Data (CLOUD) Act (enacted in March 2018), and India's Intermediary Guidelines and Digital Media Ethics Code (enacted in 2021). By analyzing policies of various countries and the diverse stances of stakeholders including government agencies, service providers and users, researchers, and global regulatory organizations. This study encourages readers to consider how legal frameworks might evolve to address the tensions between privacy, security, and public safety in the digital age.

Analysis

Telegram has emerged as a central platform in encryption policy debates due to its widespread adoption and technically robust architecture. As of 2025, it ranks as the fourth most used messaging platform globally, appealing to users seeking enhanced privacy and unregulated communication. Its "secret chats" feature uses end-to-end encryption (E2EE), combining industry-standard protocols such as 256-bit AES, RSA-2048, and the Diffie-Hellman key exchange algorithm. (These sophisticated encryption methods hinder law enforcement efforts, a situation commonly referred to as the “going dark” phenomenon.) This technological evolution severely restricts access to critical digital evidence necessary for criminal investigations (Comey, 2014)

Telegram also provides self-destructing messages, which erase themselves after a set duration, private channels that can host thousands of users anonymously, and pseudonymous account creation, requiring only a phone number that can be easily anonymized through virtual services. These features, designed to protect user privacy and anonymity, inadvertently facilitate cybercriminal activities by significantly complicating law enforcement surveillance and

investigative efforts. Specifically, self-destructing messages hinder the preservation of digital evidence, while pseudonymous and anonymous channels obstruct user identification, effectively allowing criminals to operate without fear of detection (Dargahi Nobari, Sarraf, Neshati, & Daneshvar, 2020). According to research, the combination of these privacy features directly contributes to a rise in cybercriminal behavior by providing a secure and low-risk environment for illicit activities (Roy et al., 2024). In May and June 2024 alone, there was a 53% surge in Telegram posts related to cybercriminal activities compared to the same period the previous year ("Cybercriminal Activity on Telegram," 2024). Moreover, a recent study analyzed 339 cybercriminal channels on Telegram, collectively followed by over 23.8 million users, underscoring how these technical characteristics facilitate widespread dissemination of compromised credentials, pirated software, hacking tools, and other malicious resources (Roy et al., 2024). This technical design increases the difficulty and cost of criminal investigations, thus placing a substantial burden on law enforcement resources.

The "going dark" issue is deeply rooted in the technical design of modern encryption systems. Device-level encryption—such as Apple's Secure Enclave or Android's Titan M chip—integrates encryption keys directly into hardware, meaning that even the manufacturers cannot retrieve user data without the user's password. (These security measures are effective in protecting personal information but also limit lawful investigative access. The infamous San Bernardino shooting case in 2016 illustrated this limitation vividly: the FBI was unable to access the perpetrator's encrypted iPhone and had to spend $1.3 million on third-party tools with limited efficacy. Similar challenges persist in 2025, with law enforcement agencies increasingly relying on costly and legally ambiguous gray-market hacking tools.

Cloud-based encryption introduces another layer of complexity. Services like Google Drive and Apple's iCloud offer encrypted data storage, but jurisdictional hurdles often obstruct access due to conflicting international legal frameworks governing data privacy and transfer. For instance, data stored by U.S.-based service providers might be subject to U.S. law enforcement requests under the CLOUD Act, yet simultaneously be protected under stricter data privacy laws like the European Union's General Data Protection Regulation (GDPR), creating a legal impasse. The U.S. CLOUD Act of 2018 was designed to streamline cross-border data access; however, it conflicts with international data protection regimes such as the EU's GDPR, limiting its effectiveness. A 2024 report by the Department of Justice indicated that 43% of iCloud data requests resulted in partially recovered or completely inaccessible files due to client-side encryption protocols.

Telegram, however, exemplifies the most challenging case for investigators. Unlike other messaging apps that backup messages to the cloud, Telegram's secret chats are strictly device-local. Combined with the use of self-destruct timers and ephemeral metadata, this architecture offers virtually no trail for law enforcement to follow. Investigators cannot subpoena data that does not exist. As encryption standards improve and quantum-resistant algorithms emerge, these technical hurdles are likely to deepen, unless balanced by responsive policy adaptations. Recognizing the growing challenges posed by encryption, countries have adopted varying legal responses, shaped by cultural, political, and legal traditions. In the US, the Department of Justice has promoted initiatives such as "Responsible Encryption," a concept proposing the creation of secure encryption that allows access only with judicial authorization (Rosenstein, 2017). However, this proposal requiring security backdoors has not been well received among both security experts and major tech companies. This kind of exceptional-access

scheme presents significant, intractable information security, economic, and public-safety risks. Yet it cannot guarantee that law enforcement will actually be able to obtain plaintext messages or device data in all cases (Pfefferkorn, 2018).

In 2018, the United States also enacted the Clarifying Lawful Overseas Use of Data (CLOUD) Act for fast accessing data held by the U.S.-based providers that are critical to investigations of serious crime, ranging from terrorism and violent crime to sexual exploitation of children and cybercrime (U.S. Department of Justice, 2023). However, the major issue with the CLOUD Act is its conflict with the European Union's General Data Protection Regulation (GDPR). The GDPR is a privacy and security law enacted in 2018 that imposes obligations on organizations that target or collect data related to people in the EU (GDPR.eu, n.d.).

The CLOUD Act, as codified in U.S. federal law, states that providers of electronic communication or remote computing services must comply with lawful requests to preserve, back up, or disclose user data in their possession or control, regardless of whether the data is stored within or outside of the United States (18 U.S.C. § 2713, 2018). In contrast, the GDPR prohibits data controllers or processors from transferring personal data to third countries unless certain conditions are met (La Scala, 2019). (This regulatory discord places companies operating in Europe—particularly those affiliated with U.S providers—in a tricky legal position.) If these companies do not comply with the CLOUD Act, they will run afoul of US law. On the other hand, if they decide to comply with the data transfer requests, they could face huge fines for violating the GDPR (DiGiacomo, 2019).

A recent example of this conflict occurred in May, 2023. Meta Platforms Ireland Limited (Meta IE) was issued a 1.2 billion euro fine following an inquiry into its Facebook service, by

the Irish Data Protection Authority (IE DPA). This fine was the largest GDPR fine ever and was imposed for Meta's transfers of personal data to the U.S. Meta also has been ordered to bring its data transfers into compliance with the GDPR (European Data Protection Board [EDPB], 2023).

In the United States, policy debates have been highly polarized between the government security agencies and technical experts, with little progress in achieving a functional compromise. Attempts such as the "EARN IT Act" have sought to curtail the immunity provided under Section 230(c)(1) of the Communications Decency Act, which states that "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider" (47 U.S.C. § 230(c)(1), 1996). The EARN IT Act proposes to deny this protection to platforms that fail to take sufficient measures against CSAM (Child Sexual Abuse Material) (EARN IT Act of 2023, S.1207, 118th Congress). Despite being introduced three times, the bill has not yet been enacted into law. Similarly, various state-level encryption access bills have also faltered due to concerns over constitutional rights and technical infeasibility. The lack of a unified national encryption policy has led to fragmentation, where federal, state, and private actors operate with conflicting objectives.

Australia also enacted the Telecommunications and Other Legislation Amendment (TOLA) Act in December 2018. This act authorizes the Director-General of Security or the chief officer of an interception agency to issue a Technical Assistance Notice (TAN), requiring communications providers to perform certain acts listed in Section 317E—such as removing one or more forms of electronic protection or providing technical information, and installing, maintaining, testing or using software—if the acts are directly related to objectives outlined in Section 317L(2)(c), including safeguarding national security, enforcing criminal law related

serious Australian offences, or assisting the enforcement of the criminal laws in a foreign country (Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, 2021).

However, many organizations, including IEEE and the European Union Agency for Cybersecurity (ENISA), along with privacy law and cybersecurity experts have expressed concerns that systemic weaknesses created by introducing exceptional access and decryption could create more opportunities for hackers' attacks and weaken public trust. It is also pointed out that the definition and guidance of the Act are vague and not practical to achieve what the Act is designed for. In response to such opposing arguments, Mike Burgess, the Director-General of the Australian Signals Directorate, stated, "Systemic weaknesses are explicitly prohibited by the Act, with an analogy of entering a locked room in a hotel for anti-terrorist purposes and not demanding a master key for all rooms" (Burgess, 2018).

Australia's ability to swiftly enact such a law is largely attributed to its parliamentary system, where the ruling coalition can fast-track legislation with limited procedural barriers or bipartisan gridlock (Hardy, 2020). This political structure stands in contrast to the United States, where a bicameral legislature and deeply entrenched partisan divides often hinder the passage of surveillance-related bills. Furthermore, unlike the U.S., where strong constitutional protections under the First and Fourth Amendments provide a robust legal shield for privacy and free expression, Australia lacks comparable constitutional safeguards, allowing greater latitude in expanding surveillance powers (Karp, 2018).

Australia's TOLA Act is often cited as a case of overreach. Although it was established to empower law enforcement and national security agencies for the sake of public security, it

couldn’t avoid criticism for harming the brand image and trust in service providers. * Since there has not been any significant public research that attempts to quantify the economic impact of TOLA and there are challenges of estimating the potential economic loss due to TOLA, the lack of such empirical evidence does not imply that there is no significant impact. In a survey of 79 companies, around 20% reported that the law had negatively affected their business, while a further 21% believed that TOLA would increase their future operating costs due to compliance and remediation obligations. One company estimated a direct adverse economic impact of approximately AU$1 billion as a result of the Act (Barker et al., 2021).

In the case of India, the Ministry of Electronics and Information Technology introduced IT rules mandating that social media intermediaries providing messaging services must have the technical capability to identify the “first originator” of a message upon request from a competent authority or a court order (Intermediary Guidelines and Digital Media Ethics Code, 2021). Under this framework, a company like WhatsApp could be compelled to disclose the identity of the first user who disseminated a particular message related to a terrorism investigation, even if the content of the message remains encrypted. In response, WhatsApp filed a constitutional lawsuit against the Indian government in 2021 (Ellis-Petersen, 2021).

India’s policy model represents a more forceful approach. The legal battle between India’s government and WhatApp is still ongoing. (This has not only raised red flags among human rights organizations but also discouraged foreign investment and innovation in the Indian tech sector.) WhatsApp's legal representative expressed significant concerns, saying that the company might consider exiting the Indian market if compelled to compromise the encryption that protects users' messages. The platform's commitment to user privacy, underscored by its end-to-end encryption, forms the core of its user trust and appeal (India Today Tech, 2024).

Despite their combined efforts, government and law enforcement entities throughout these jurisdictions continue to face obstacles when addressing encryption-related problems because diverse stakeholder interests conflict with each other. Governments prioritize national security and law enforcement access, while technology companies and standard-setting organizations put more value on user privacy and cybersecurity integrity. (These competing priorities make it difficult to establish definitive solutions.)

Conclusion

Addressing the encryption conundrum requires comprehensive and cooperative solutions involving multiple stakeholders. Encryption will continue to grow stronger, and accessing encrypted content without user cooperation may become virtually impossible. Nevertheless, progress is possible if each stakeholder fulfills their responsibilities within their respective domains.

Engineers should proactively integrate ethical considerations into the design of encryption systems to minimize their misuse while safeguarding user privacy. Technical strategies like lawful hacking present potential pathways to enabling law enforcement access without weakening encryption systems (Bellovin et al., 2018). Another viable approach is the use of homomorphic encryption (HE), a cryptographic technique that addresses a critical challenge in information security, particularly in cloud computing environments where sensitive data processing is essential. With HE, encrypted values E(a) and E(b) can be computed to E(a+b) without decryption, maintaining data privacy throughout the entire process (Yi et al., 2014). HE offers a promising solution to protect users' accounts and assets from malicious third parties

while also offering a method for law enforcement to access necessary information without infringing on user privacy. This approach effectively mitigates risks associated with untrusted providers retaining sensitive data and user credentials long after the service relationship ends (Acar et al., 2018).

Lawmakers must invest in technical literacy and seek expert consultation before drafting and enacting encryption-related legislation, ensuring policies are both practical and technically feasible. Furthermore, international cooperation is critical, necessitating global regulatory frameworks achieved through collaborative negotiation to address conflicts such as those between the CLOUD Act and GDPR. These reciprocal legal conflicts arise because both the U.S. and EU assert extraterritorial jurisdiction over data access while simultaneously enforcing blocking statutes that prohibit disclosure to foreign authorities. Without new bilateral agreements or multilateral frameworks, these legal contradictions will continue to obstruct law enforcement's ability to access critical digital evidence across borders (Shurson, 2020).

By pursuing these multidimensional strategies, it is possible to find an effective balance between protecting individual privacy, ensuring cybersecurity, and maintaining public safety.

Reference

Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Green, M., Landau, S., Neumann, P. G., Rivest, R. L., Schiller, J. I., Schneier, B., Specter, M., & Weitzner, D. J. (2015). Keys under doormats: Mandating insecurity by requiring government access to all data and communications. Journal of Cybersecurity, 1(1), 69–79. https://doi.org/10.1093/cybsec/tyv009

Acar, A., Aksu, H., Uluagac, A. S., & Conti, M. (2019). A Survey on Homomorphic Encryption Schemes: Theory and Implementation. ACM Computing Surveys, 51(4), Article 79. https://doi.org/10.1145/3214303

Burgess, M. (2018). Director-General ASD statement regarding the TOLA Act 2018. Australian Signals Directorate. https://www.asd.gov.au/news-events-speeches/speeches/director-general-asd-statement-regarding-tola-act-2018

Buresh, D. L. (2021). The Battle for Backdoors and Encryption Keys. Journal of Current Scientific Research, 1(3), 13–22. https://doi.org/10.14302/issn.2766-8681.jcsr-21-3789

Comey, J. B. (2014, October 16). Going dark: Are technology, privacy, and public safety on a collision course? Brookings Institution. https://archives.fbi.gov/archives/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course

Dargahi Nobari, A., Sarraf, M., Neshati, M., & Daneshvar, F. (2020). Characteristics of viral messages on Telegram; The world's largest hybrid public and private messenger. Expert Systems with Applications, 168, 114303. https://doi.org/10.1016/j.eswa.2020.114303

DiGiacomo, J. (2019, September 30). Cloud Act Compliance & Relationship to GDPR. Revision Legal. https://revisionlegal.com/internet-law/cloud-act-compliance-relationship-to-gdpr/

European Data Protection Board. (2023, May 22). Binding Decision 1/2023 on the dispute submitted by the Irish SA on data transfers by Meta Platforms Ireland Limited for its Facebook service (Art. 65 GDPR). https://edpb.europa.eu/our-work-tools/our-documents/binding-decision/binding-decision-12023-dispute-submitted-irish-sa-data_en

Fleckenstein, M., Obaidi, A., & Tryfona, N. (2023). A review of data valuation approaches and building and scoring a data valuation model. Harvard Data Science Review, 5(1). https://doi.org/10.1162/99608f92.c18db966

GDPR.eu. (n.d.). What is GDPR, the EU's new data protection law? https://gdpr.eu/what-is-gdpr/

Hardy, K. (2020). Australia's encryption laws: practical need or political strategy? Internet Policy Review, 9(3). https://doi.org/10.14763/2020.3.1493

Hartel, P., & van Wegberg, R. (2023). Going dark? Analysing the impact of end-to-end encryption on the outcome of Dutch criminal court cases. Crime Science, 12(5). https://doi.org/10.1186/s40163-023-00185-4

H.R.6544 - 117th Congress (2021-2022): EARN IT Act of 2022. (2022, February 2). https://www.congress.gov/bill/117th-congress/house-bill/6544

Karp, P. (2018, December 7). Australia's war on encryption: The sweeping new powers rushed into law. The Guardian. https://www.theguardian.com/technology/2018/dec/08/australias-war-on-encryption-the-sweeping-new-powers-rushed-into-law

La Scala, G. (2019, November 14). CLOUD Act vs. GDPR: United States and European Union clash over data protection. Fordham International Law Journal. https://www.fordhamilj.org/iljonline/united-states-and-european-union-clash-over-data-protection

Manpearl, E. (2017). Preventing “Going Dark”: A sober analysis and reasonable solution to preserve security in the encryption debate. University of Florida Journal of Law & Public Policy, 28, 65–100.

Pangarkar, T. (2025, January 14). Encryption software statistics 2025 by security, algorithm, authenticity. Scoop Market. https://scoop.market.us/encryption-software-statistics/

Pfefferkorn, R. (2018, February 5). The risks of “responsible encryption”. Stanford Center for Internet and Society. https://cyberlaw.stanford.edu/publications/risks-responsible-encryption

Rosenstein, R. J. (2017, October 10). Deputy Attorney General Rod J. Rosenstein delivers remarks on encryption at the United States Naval Academy. U.S. Department of Justice. https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-encryption-united-states-naval

S.3398 - 116th Congress (2019-2020): EARN IT Act of 2020. (2020, July 20). https://www.congress.gov/bill/116th-congress/senate-bill/3398

Shurson, J. (2020). Data protection and law enforcement access to digital evidence: Resolving the reciprocal conflicts between EU and US law. International Journal of Law and Information Technology, 28(2), 167–184. https://doi.org/10.1093/ijlit/eaaa002

Stach, C. (2023). Data Is the New Oil–Sort of: A View on Why This Comparison Is Misleading and Its Implications for Modern Data Administration. Future Internet, 15(2), 71. https://doi.org/10.3390/fi15020071

Steven M. Bellovin, Matt Blaze, Sandy Clark, & Susan Landau. (2014). Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet. Northwestern Journal of Technology and Intellectual Property, 12(1), 1–43. https://scholarlycommons.law.northwestern.edu/njtip/vol12/iss1/1

U.S. Code. (1996). 47 U.S.C. § 230 – Protection for private blocking and screening of offensive material. https://www.law.cornell.edu/uscode/text/47/230

U.S. Department of Justice. (2023, October 24). CLOUD Act resources. https://www.justice.gov/dag/cloud-act-resources

Yaseen, M., & Banerjee, J. (2025). The Role of Telegram's Privacy Policies in Facilitating Cyber Crimes and Legal Challenges in Cyber Law. 4, 13–28. https://www.researchgate.net/publication/387875897_The_Role_of_Telegram's_Privacy_Policies_in_Facilitating_Cyber_Crimes_and_Legal_Challenges_in_Cyber_Law

Yi, X., Paulet, R., & Bertino, E. (2014). Homomorphic Encryption and Applications. SpringerBriefs in Computer Science. https://www.semanticscholar.org/paper/Homomorphic-Encryption-and-Applications-Yi-Paulet/4be948fc9dc533d11497a38b76f65076ffb89cbd