DS Journal of Digital Science and Technology
Volume 4 Issue 1, 1-10, Jan - Mar 2025
ISSN: 2583-5416 / https://doi.org/10.59232/DST-V4I1P101

Review Article

The Validity of Kerckhoff's Principle in the Era of Emerging Technologies: A Case Study of Cryptology in Wireless Telephony Services

Frankline Makokha

Department of Computing and Informatics, University of Nairobi, Nairobi, Kenya.

goldmedalist321@gmail.com

Received: 03 January 2025; Revised: 05 February 2025; Accepted: 10 March 2025; Published: 31 March 2025

Abstract - Cryptosystems are meant to ensure that the confidentiality, integrity, and availability of information carrying and storing medium is sustained. Various algorithms have been developed to actualize these cryptosystems. The algorithms comprise the instructions and the keys to implement the algorithms. According to Kerckhoff's Principle, the instructions should be published while the key should be kept secret. Using a Systematic Literature Review, this paper analyzed the validity of this principle because of the power of emerging technologies, focusing on cryptosystems in wireless telephony services. From the findings, all encryption algorithms used in wireless telephony services do not abide by Kerckhoff's Principle, they are proprietary and unpublished. However, this has not stopped reverse engineering the algorithms and making them public by various scientists. The algorithms have also been found to be susceptible to breach, but only in laboratory environments as proof of concept. The paper did not establish any breaches that were realized in commercial environments. Further, this paper found no causation or correlation between non-compliance with Kerckhoff's Principle and cases of compromise of the algorithms. As to whether emerging technologies pose a risk to published algorithms, this paper established that emerging technologies like Artificial Intelligence and Quantum `Computing are more inclined to strengthen existing cryptosystems through Crypto-Influenced AI (CIAI) and AI-Influenced Cryptography (AIIC) paradigms than being used to subvert them.

Keywords - AI-influenced cryptography**,** Crypto-influenced AI**,** Deep Learning, Kerckhoff's principle**,** Quantum computing.

1. Introduction

Cryptology, as a field of study, encompasses two domains, namely, cryptography and cryptoanalysis [1]. Cryptography entails hiding the presence of communication or the meaning of a communication. Cryptoanalysis involves breaking the mechanisms used to hide the presence or meaning of communication [1].

Cryptography is composed of two building blocks, namely, the algorithm and the key. The algorithm contains the procedure for converting readable message, plain text, into unreadable form, ciphertext, while the key refers to the rules to be used in converting plain text to ciphertext and vice versa [2]. Kerckhoffs' Principle of 1883, by Auguste Kerckhoff, postulates that a cryptosystem should use published, well-scrutinized algorithms and protocols while keeping the key as the only secret [3].

The significance of Kerckhoff's Law is that a cipher algorithm can fall into the hands of an enemy or any party with bad intentions without compromising the confidentiality of the information ciphered by the algorithm [4]. An

American mathematician, Claude Shannon, recast Kerckhoffs's principle into an assumption when using cryptosystems as "the enemy knows the system" [5].

The justification for this principle is that it is easier to maintain the confidentiality of the shorter keys than the algorithm, which is longer and more complex [4]. Further, in case of a key compromise, it is easier to change the key alone than to change the entire algorithm.

For large-scale deployment, it is easier for all users to use different keys but the same algorithm instead of each set of users using different algorithms [4]. Could the integrity of this law, made in the 19th century and which has been applied since then, be impacted by emerging technologies with higher computing capabilities?

Given unlimited computing power, an unrealistic assumption when the principle was first coined, such computationally secure systems could be broken, but in practice, they appear to be unbreakable, lacking tools for proving systems to be computationally secure notwithstanding [6]. However, in this century, emerging technologies render the prospect of unlimited computing power a reality.

Emerging technology refers to a new and fast-growing knowledge-producing and application field of study that considerably impacts socio-economic domains [7]. Key characteristics of emerging technologies include radical novelty, rapid growth, coherence, huge impact, uncertainty and ambiguity [7]. Artificial intelligence is one of the key emerging technologies that negatively and positively impact cyber security [8].

Machine learning algorithms, which are based on artificial intelligence, are better at providing security than humans; conversely, they also help attackers increase their knowledge to find weaknesses in cybersecurity technologies [8].

The other emerging technology likely to impact cryptosystems is Quantum computing. Unlike in classical computers, where the fundamental computing blocks take two-bit states of either 0 or 1, in Quantum computers, the computing blocks use quantum bits (qubits), which can exist simultaneously in either 0, 1 or both states, a superposition phenomenon [9].

Two qubits can be entangled, forming a single object with four different states, implying that if one of the two qubits' states changes, the entangled qubits will change, too [10]. This is due to the exponential increase in the number of values that can be processed in one operation when the number of entanglement qubits increases [10].

Superposition and entanglement are the pillars of quantum parallelism, which allows quantum computers to explore multiple possibilities simultaneously, enabling certain calculations much faster than classical computers [11].

Given the two main emerging technologies, artificial intelligence and quantum computing, there has not been an in-depth study to identify the possible negative impact of existing cryptosystems, especially regarding the Kerckhoffs' Principle.

In particular, no study focuses on the impact of the said emerging technologies on cryptosystems used in wireless telecommunications, noting that the principle was postulated before the two emerging technologies gained traction.

This paper explores the validity of Kerckhoffs' Principle in view of the emerging technologies with a focus on wireless telephony services, comprising cellular mobile networks, cordless phones, satellite phones and two-way radio communication.

In addressing the issue under study, section 2 talks about similar works that have been done with regard to the problem statement, section 3 highlights the approach used in the study, section 4 delves into various cryptographic algorithms used in wireless telephony services with a view of establishing whether they are published or unpublished. In contrast, section 5 summarises and concludes the findings.

2. Related Works

Based on the study of the Impact of Quantum Computing on Present Cryptography, it was noted that all existing cryptographic systems are considered weak against quantum computers [9]. It is postulated that quantum computers will end public key encryption schemes [12].

Of particular interest are two quantum algorithms, namely, Shor's Algorithm and Grover's algorithm, which can be used to break Asymmetric Cryptographic systems and Symmetric Cryptographic, respectively [9]. It has been shown that quantum computers reduce the effective key strength of an algorithm by more than half, and in some algorithms, the original key strength is reduced to zero [9].

Quantum-safe and quantum-vulnerable cryptographic algorithms exist, the former being secure from breach using quantum supremacy, while the latter being insecure [13]. Quantum supremacy is the ability of a quantum computer to execute a computational task that is beyond the capability of any classical computer [14].

A demonstration of quantum supremacy was in 2019 when a group of researchers at Google published a paper stating that they created a quantum processor that carried out a specific calculation in 200 seconds, which would otherwise take 10,000 years [15].

In 2020, a group of researchers at the University of Science and Technology of China (USTC) demonstrated that their quantum computer generated a certain number of samples in 20 seconds, which would take 600 million years for a classical supercomputer [15].

In 2020, a successful proof of concept of a collision attack against the hashing algorithm was performed using quantum computers [16]. Shor's algorithm running on a large-scale quantum computer was shown to breach prime factorization for number 21 in 2012 [17].

Deep learning, a machine learning technique in the context of side-channel attacks, has been used in experiments that yield successful key recovery [18]. The experiment used different feature extraction methods and exploited samples' time dependency.

Deep learning refers to automatically and progressively deriving insights from multiple levels of representations of the underlying distribution of the data [19]. In deep learning, initial layers extract low-level features, and succeeding layers combine features to form a complete representation [20].

Deep learning can play a significant role in breaking cryptosystems based on the type of attack at play. Attacks on cryptosystems can take five forms: Ciphertext only attack, Known Plaintext attack, Chosen Plaintext, Chosen Ciphertext and Chosen Text [21]. It has been shown that it is possible to attack the three main cryptographic algorithms used in GSM mobile networks. Namely, A5 is used for encryption, A3 is used for authentication, and A8 is used for key agreement [22].

The relationship between cryptography and Artificial Intelligence (AI) has been split into two themes, namely, Crypto-Influenced AI (CIAI) and AI-Influenced Cryptography (AIIC) [23]. When AI models provide chaos, randomness, and many other properties, all of which are required by cryptosystems, the resultant cryptosystem is termed AIIC, while if AI evolves by inculcating the concepts of cryptography into it, the resultant AI system is termed as Crypto-Influenced AI (CIAI) [24].

AIIC evolves through five stages: AI-Unaware Cryptography (AIUC), during which cryptography is vulnerable to Machine Learning (ML) and Deep Learning (DL) attacks; AI-Resilient Cryptography (AIRC), wherein cryptosystems adopt caution towards ML and DL attacks; AI-Boosted Cryptography (AIBC) cryptographic techniques, protocols, methods, devices, etc., are supported by AI models; AI-Assisted Cryptography (AIAC) where AI is utilized by one or more of the internal components of the cryptosystem, and directly for cryptographic purposes, and AI-Embedded Cryptography (AIEC) AI is used by the encryption/decryption component [24].

In the study on the existence of cryptography in Instance Messaging, four key metrics, namely, Avalanche Effect, Randomness, Test Key Space, and Kerckhoff's Principle, were used in evaluating the best cryptographic algorithm for use in Instant Messaging to ensure the confidentiality of sent messages [25]. The avalanche effect refers to a property of an encryption algorithm where a minor change in the plaintext results in a mega change in the ciphertext [26].

Randomness refers to the property of an algorithm to produce an outcome from a probabilistic process that produces independent, uniformly distributed and unpredictable values that cannot be reliably reproduced [27]. Randomness is, therefore, characterised by unpredictability, independence of values (lack of correlation) and uniform distribution (lack of bias).

Test Key Space is a set of possible keys that can encode data using a given algorithm [28]. The same authors postulate that a strong encryption scheme should have a large key space to be tried in any brute-force attack on that technique. It was noted that adherence to Kerckhoff's Principle was the least important in determining the best cryptographic algorithm compared to the rest of the metrics [25].

Prior work on the validity of Kerckhoff's Principle exists. However, it falls short in linking the principle to actual breaches in commercial deployments caused by not publishing the encryption algorithm and whether emerging technologies negatively impact the principle. This paper, therefore, addresses whether publishing the algorithm impacts the strength of the cryptosystem in view of emerging technologies, with a focus on wireless telephony services.

3. Materials and Methods

This paper uses a Systematic Literature Review approach to identify the main cryptographic algorithms used in wireless telephony services, establishing whether they are published as per Kerckhoff's Principle. A Systematic Literature Review (SLR) is a transparent and reproducible methodical approach to solving a given research question through exhaustive synthesis and appraisal of the quality of published scientific evidence on the topic [29]. The Systematic Literature Review method requires eligibility criteria, literature sources, search strategy, and synthesis methods to be defined in a priori [30].

In this paper, the literature to be reviewed was from papers published in peer-reviewed and refereed journals. The search was conducted on Google Scholar since it is a free platform, and there was no specification on the year of article publication for reviewing as much published literature as is available. The search strategy involved grouping the search criteria into four thematic areas: General Topics, Algorithm-Specific Searches, Vulnerability-Focused and Emerging Technologies-Focused.

The search texts under General Topics were: "Validity of Kerckhoffs' Principle on Cryptography"," Impact of Artificial Intelligence on Kerckhoffs' Principle", and "Impact of quantum computing on Kerckhoffs' Principle".

The texts used in Algorithm-Specific Searches were: "Cryptographic algorithms in GSM, 3G, 4G, 5G, satellite phones, DECT, trunked radio". The search text for Vulnerability-Focused searches was: "Attacks on GSM cryptographic algorithm", while the search text for Emerging Technologies-Focused was: "Impact of quantum computing on Kerckhoffs' Principle" and "Artificial Intelligence-driven attacks on wireless telephony services". An analysis was then done to establish whether emerging technology enhanced the reported attacks that meet the search criteria or if it was actualized using classical attack methods.

For information on general publicly reported attacks on wireless telephony services, search texts were typed directly on the Google platform, and an analysis was done to establish the dominant causes of breaches in the networks. The search text was “Who has been hacked 2024”.

The data from this search was sieved for only data relating to telecommunication companies. The collected literature was then analysed qualitatively and quantitively to identify causation and correlation links. Table 1 summarizes the research design search criteria.

Table 1. Systematic literature review design

Thematic Area	Search Text
General Topics	⇒ Validity of Kerckhoffs' Principle on Cryptography ⇒ Impact of Artificial Intelligence on Kerckhoffs' Principle ⇒ Impact of quantum computing on Kerckhoffs' Principle
Algorithm-Specific Searches	⇒ Cryptographic algorithms in GSM, 3G, 4G, 5G, satellite phones, DECT, trunked radio
Vulnerability-Focused	⇒ Attacks on the GSM cryptographic algorithm ⇒ Artificial Intelligence-driven attacks on wireless telephony services
Emerging Technologies-Focused	⇒ Impact of quantum computing on Kerckhoffs' Principle

4. Results and Discussion

Global System for Mobile Communication (GSM) uses A3, A5 and A8 cryptographic algorithms for security [31]. A3 is used for subscriber authentication, A5 is used for ciphering and deciphering user data, and A8 is used for cipher key generation. The three algorithms are proprietary [32] and do not adhere to Kerckhoff’s Principle. The COMP128 implementation used in GSM networks as an instantiation of two proprietary algorithms, A3 and A8, was shown to be vulnerable to cryptographic attack where the 128-bit key could be extracted using as few as 8 chosen plaintexts [33].

The A5 stream cipher, the secret and proprietary algorithm used for encryption of the data transmitted between the mobile device and the Base Transceiver Station (BTS), was shown to be susceptible to a ciphertext-only attack [34]. Version 3 of the A5, A5/3 (KASUMI), developed by the 3rd Generation Partnership Project (3GPP), was proprietary yet published [35]. It was shown that the A5/3 is vulnerable to related key attacks and higher order differential attacks [36].

In GPRS technology, protecting against eavesdropping between the phone and the base station involves a stream cipher that uses two proprietary encryption algorithms, GPRS Encryption Algorithm, GEA-1 and GEA-2 [37]. However, it was shown that eavesdropping and reverse engineering is possible for the GPRS algorithms [38]. Cellular and fixed telephony networks use the Signalling System (SS7) protocol to set up and tear down calls, providing cellular roaming, messaging, and monitoring services [39]. With the evolution of networks to IP, a set of signalling transport protocols called SIGTRAN, an extension to SS7 that allows the use of IP networks to transfer messages, was developed [40].

Access to SS7 and one's phone number makes it possible to listen to a conversation, locate one's whereabouts, wiretap messages, and even access mobile financial services, and execute Unstructured Supplementary Service Data (USSD) commands [40]. To enhance Authentication Authorization and Auditing in 4G networks, 3GPP chose a diameter for signalling and AAA provisioning in 4G and all next-generation mobile networks [41].

However, experiments have shown that Diameter is still vulnerable and can be used for privacy breaches and denial of service attacks, which, again, can be countered by IPsec and SMS home routing if configured by mobile operators [41]. In 5G networks, due to advanced features and architecture, like Control and User Plane Separation (CUPS), Service Based Architecture (SBA), Network Slicing (NS) and Access Agnostic, HTTP/2 is used as application layer protocols; thus, all the network entities in control plane will communicate with each other using HTTP/2 [42].

The 5G HTTP/2 signalling also presents its own weaknesses, ranging from broken service access control, which occurs through token-based authorization through OAuth 2.0. This exposes the 5G network to token tampering attacks and API Exploitation since APIs are exposed to all endpoints within the same network or with roaming partners [43]. Other protocols, like Radio Resource Control (RRC), a layer 3 (Network Layer) protocol used between UE and Base Station in 3G, LTE and 5G cellular networks, were found to be vulnerable, despite it being published by 3GPP [44].

To counter the 5G HTTP/2 signalling threats, Machine Learning (ML) and Artificial Intelligence (AI) techniques can be leveraged for intelligent threat analysis and detection [43]. Another wireless telephony service, cordless phones, involves using a low-cost, low-mobility wireless link replacing the cord connecting a telephone base unit and its handset [45]. The two standards for cordless phones are Digital Enhanced Cordless Telecommunications (DECT) for the European Market and Personal Handyphone System (PHS) from Japan and the Asian Market, which supports handover using telepoints mounted in busy areas. Where people congregate [45], another standard, the Personal Access Communications System (PACS), was developed in the United States [46].

Digital Enhanced Cordless Telecommunications (DECT) has two main algorithms: DECT Standard Cipher (DSC), which encrypts the communication and protects the confidentiality of the conversation, and DECT Standard Authentication Algorithm (DSAA), which authenticates a DECT phone and is designed to protect against an adversary that tries to piggyback on someone else's telephone connection [47].

DSC and DSAA were shown to have vulnerabilities that allow a correlation attack on the cipher, which allows the decryption of an intercepted call and impersonation of a BTS and performs a relay attack, respectively [48]. The two algorithms are proprietary. However, their public descriptions and cryptanalytic results on their components have been given [47]. The other means of actualizing wireless telephony service, Satellite systems, comprises mobile or fixed equipment on the earth's surface, termed earth stations and other equipment orbiting the earth called space stations [49]. The configuration architectures of Satellite systems take the form of Fixed-Satellite Services (FSS), where the earth station is fixed, and Mobile-Satellite Services (MSS), where the earth station is portable, and intersatellite, which involves satellite-to-satellite links [49] like in satellite phones. Cryptographic algorithms used in satellite phones, GMR-1 and GMR-2, are proprietary and have been shown to be vulnerable to ciphertext-only attacks and known plaintext attacks, respectively [50].

In two-way radio communications, also called Land Mobile Radio, there exists two system configurations, namely, conventional system, where a frequency band is permanently dedicated to a voice channel, and trunked system, where a pool of frequencies are assigned on demand to a group of users (talk group) and released at end communication [51]. Among the digital radio trunk systems that International Standards Organizations have standardized are Terrestrial Trunked Radio (TETRA), Project 25 (P25) and Digital Mobile Radio (DMR) [51].

TETRA Encryption Algorithm (TEA), a suite of encryption algorithms associated with Terrestrial Trunked Radio (TETRA), a European standard for public safety and emergency services, standardized by the European Telecommunications Standards Institute (ETSI), is used for the encryption of voice and data traffic on a TETRA radio network, were reverse engineered and extracted isolated and analysed from a working TETRA radio [52].

Digital Voice Protection (DVP), a proprietary self-synchronising algorithm for the encryption and decryption of voice communication from Motorola Inc., despite being unpublished, was reverse-engineered from the custom-developed cryptographic chip and its firmware and simulation of the algorithm in software proved that it could be broken in real-time [53]. The GSMA Mobile Telecommunications Security Landscape Report of February 2024 shows that the attack surface of Mobile telecommunications networks has become wide and complex, occasioned by IoT devices, new 5G standalone cores, network Application Programming Interfaces (APIs), open-Radio Access Network (RAN) architectures and new artificial intelligence-enabled services [54].

The report shows the main attacks as data breaches, ransomware attacks, supply chain attacks, reconnaissance and initial access, direct attacks on service delivery, DDOS attacks, social engineering, and compromising 'the edge'. From the report, attacks occasioned by the compromise of cryptographic algorithms are not common or non-existent. On the internet, there exist several companies that summarize various breaches in the telecom industry throughout the year, among them Wisdiam, SoCRadar, GSMA and Cyber Security Ventures.

Data from the three entities pointed out telecom infrastructure sabotage involving cutting long-distance cables and general vandalism, theft of customer data through a data breach, ransomware, Distributed Denial of Service (DDoS) and Social Engineering practices geared towards breaching customer data as the main cyber attacks on telecom infrastructure. Table 2 summarises the identified algorithms and Kerchoff's principle compliance status.

Table 2. Systematic literature review design

Technology / Network Generation	Algorithms	Compliance with Kerckhoffs' Principle
GSM	A3, A5 and A8 Cryptographic Algorithms	Non Complaint (proprietary and unpublished)
GPRS	GPRS Encryption Algorithm, GEA-1 and GEA-2	Non-compliant (proprietary and unpublished)
Signalling System (SS7)	SS7 protocol, SIGTRAN, Diameter, HTTP/2 and Radio Resource Control (RRC)	Complaint (proprietary but published)
Digital Enhanced Cordless Telecommunications (DECT)	DECT Standard Authentication Algorithm (DSAA), DECT Standard Cipher (DSC)	Complaint (proprietary but published)
Satellite Systems	GEO-Mobile Radio Interface GMR-1 and GMR-2	Non Complaint (proprietary and unpublished)
Two Way Radio communications	Digital Voice Protection (DVP)	Non Complaint (proprietary and unpublished)

From the Systematic Literature Review, it is established that 100% of the reviewed cryptographic systems used in wireless telephony systems are proprietary. Only 30% of the reviewed cryptographic systems are published. This has, however, not stopped reverse engineering and, therefore, established the logic in the proprietary crypto algorithms.

Despite the proof of concepts in laboratories for attacks on the proprietary GSM, Satellite, Cordless Phones and Two Way Radio communications cryptographic algorithms, no reported compromise in their commercial deployments is attributed to attacks on the cryptographic algorithms.

Further, the proof of concept attacks are not attributable to or have been made easy by any emerging technologies. In any case, emerging technologies are helping to strengthen cryptographic systems through Crypto-Influenced AI (CIAI) and AI-Influenced Cryptography (AIIC), contrary to postulations that they may aid in compromising cryptosystems.

5. Conclusion

Therefore, no causation and correlation can be established that would link non-adherence to Kerckhoffs's Principle to reported cyber attacks on wireless telephony systems. Neither is there a causation and correlation that can be postulated on the fact that adherence to Kerckhoff's Principle will render the wireless telephony systems even stronger since, in any case, those proprietary cryptographic algorithms have been reverse-engineered and their logic made public.

However, this paper's findings are limited because the data collected and analysed is based purely on published information in journals and, in a few instances, on information available on the internet.

Future studies could be performed on AI-Influenced Cryptography (AIIC) to ascertain the net impact of AI on Cryptography and establish whether AI-influenced Cryptographic systems are still susceptible to attacks in laboratory environments and commercial deployments.

References

[1] Amit Kumar et al., ”Cryptography and its Components,” *International Journal for Technological Research in Engineering*, vol. 7, no. 4, pp. 6314-6316, 2019. [Publisher Link]

[2] Debabrata Samanta et al., ”Cipher Block Chaining Support Vector Machine for Secured Decentralized Cloud Enabled Intelligent IoT Architecture,” *IEEE Access*, vol. 9, pp. 98013-98025, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[3] Seungjoo Kim, Masahiro Mambo, and Yuliang Zheng, “Rethinking Chosen-Ciphertext Security under Kerckhoffs’ Assumption,” *Topics in Cryptology - CT-RSA* , 2003. [CrossRef] [Google Scholar] [Publisher Link]

[4] Jonathan Katz, and Yehuda Lindell, *Introduction to Modern Cryptography*, CRC Press, Taylor and Francis Group, Boca Raton, FL, United States, 2015. [Publisher Link]

[5] Neelanjan Manna, “ Is Kerckhoffs's Principle Still Justified?,” *International Journal of Research Publication and Reviews*, Vol. 3, no. 10, pp. 1076-1077, 2022. [Publisher Link]

[6] Martin E. Hellman, “The Mathematics of Public-Key Cryptography,” *Scientific American*, vol. 241, no. 2, pp. 146-157, 1979. [Google Scholar] [Publisher Link]

[7] Daniele Rotolo, Diana Hicks, and Ben R. Martin , “What is an Emerging Technology ?,” *Research Policy*, vol. 44, no. 10, pp. 1827-1843, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[8] M.F. Ansari et al., “The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review,” *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 11, no. 9, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[9] Vasileios Mavroeidis et al., “The Impact of Quantum Computing on Present Cryptography,” *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 3, pp. 405-414, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[10] Richard Jozsa, *Entanglement and Quantum Computation in Geometric Issues*, The Foundations of Science, Oxford University Press, 1997. [Google Scholar] [Publisher Link]

[11] Anthony Lawrence Paul, “The Impact of Quantum Computing on Cryptographic Systems,” 2024.

[12] Lily Chen et al., “Report on Post-Quantum Cryptography,” *National Institute of Standards and Technology Internal Report 8105*, 2016. [CrossRef] [Publisher Link]

[13] Matthew Campagna et al., *Quantum Safe Cryptography and Security: An Introduction, Benefits, Enablers and Challenges*, European Telecommunication Standards Institute (ETSI), France, ETSI White Paper, no. 8. 2015. [Publisher Link]

[14] Aram W. Harrow, and Ashley Montanaro, ”Quantum Computational Supremacy,” *Nature*, vol. 549, no. 7671, pp. 203-209, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[15] Frank Arute et al., “Quantum Supremacy Using a Programmable Superconducting Processor,” *Nature*, 574, pp 505–510, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[16] Akinori Hosoyamada, and Yu Sasaki, “Finding Hash Collisions with Quantum Computers by Using Differential Trails with Smaller Probability than Birthday Bound,” *Advances in Cryptology - EUROCRYPT*, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[17] Enrique Martín-López et al., “Experimental Realization of Shor's Quantum Factoring Algorithm Using Qubit Recycling,” *Nature Photonics*, vol. 6, no. 11, pp. 773-776, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[18] Houssem Maghrebi, Thibault Portigliatti, and Emmanuel Prouff, “Breaking Cryptographic Implementations Using Deep Learning Techniques,“ *The International Association for Cryptologic Research*, 2016. [Google Scholar] [Publisher Link]

[19] Francis Quintal Lauzon, ”An introduction to Deep Learning,” *11th International Conference on Information Science, Signal Processing and their Applications*, Montreal, QC, Canada, pp. 1438-1439, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[20] Amitha Mathew, P. Amudha, and S. Sivakumari, “Deep Learning Techniques: An Overview,” *Advanced Machine Learning Technologies and Applications*, Springer, Singapore, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[21] William Stalling, *Cryptography and Network Security Principles and Practice*, 5th Ed., Prentice Hall, New York, USA, 2011. [Publisher Link]

[22] Elad Barkan, Eli Biham, and Nathan Keller, “Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication,” *Advances in Cryptology-CRYPTO 2003*, Springer, Heidelberg, pp. 600-616, 2003. [CrossRef] [Google Scholar] [Publisher Link]

[23] Behrouz Zolfaghari, and Takeshi Koshiba, “AI Makes Crypto Evolve,” *Applied System Innovation*, vol. 5, no. 4, pp. 1-33, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[24] Behrouz Zolfaghari et al., “ Crypto Makes AI Evolve, *arXiv Preprint*, 2022. [Google Scholar] [Publisher Link]

[25] Vania Beatrice Liwandouw, and Alz Danny Wowor, “The Existence of Cryptography: A Study on Instant Messaging,” *4th Information Systems International Conference, Procedia Computer Science*, Bali, Indonesia, vol. 124, pp. 721-727, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[26] Rohit Verma, and Aman Kumar Sharma, “Cryptography: Avalanche Effect of AES and RSA,” *International Journal of Scientific and Research Publications*, vol. 10, no. 4, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[27] Bruice Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd Edition, John Wiley and Sons, 1996. [Google Scholar] [Publisher Link]

[28] David S. Monaghan et al., “Key-Space Analysis of Double Random Phase Encryption Technique “, *Applied Optics*, vol. 46, no. 26, pp. 6641-6647, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[29] Guillaume Lame, “Systematic Literature Reviews: An Introduction”, *Proceedings of the Design Society: International Conference on Engineering Design*, vol. 1, no. 1, pp 1633-1642, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[30] Alessandro Liberati et al., The PRISMA Statement for Reporting Systematic Reviews and Meta-Analyses of Studies That Evaluate Health Care Interventions: Explanation and Elaboration, *BMJ*, vol. 339, pp. 1-27, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[31] Bum-Sik Kim, and In-Chul Shin, “A New Authentication and Message Encryption Algorithm for Roaming Users in GSM Networks, “ *Proceedings of ITC-CSCC*, Pusan, Korea, pp. 961-964, 2000. [Google Scholar] [Publisher Link]

[32] Ren-Junn Hwang, and Feng-Fu Su, “Cryptanalysis on Stream Ciphers for GSM Networks”, *International Journal of Internet Protocol Technology*, vol. 1, no. 1, pp. 30-33, 2005. [CrossRef] [Google Scholar] [Publisher Link]

[33] J.R. Rao et al., “Partitioning Attacks: or How to Rapidly Clone Some GSM Cards”, *IEEE Symposium on Security and Privacy*, Berkeley, CA, USA, pp. 31-41, 2002. [CrossRef] [Google Scholar] [Publisher Link]

[34] Thomas Pornin, and Jacques Stern, “Software-Hardware Trade-Offs: Application to A5/1 Cryptanalysis," *Cryptographic Hardware and Embedded Systems - CHES 2000 Second International Workshop*, Worcester, MA, USA, pp. 318-327. SpringerVerlag, 2000. [CrossRef] [Google Scholar] [Publisher Link]

[35] Mitsuru Matsui, “New Block Encryption Algorithm Misty”, *Fast Software Encryption 4th International Workshop, FSE'97*, Haifa, Israel, pp. 54-68, 1997. [CrossRef] [Google Scholar] [Publisher Link]

[36] Nobuyuki SUGIO et al., “A Study on Higher Order Differential Attack of Kasumi,” IEICE *Transactions on Fundamentals*, vol. E90-A, no.1 pp. 14-21, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[37] Christof Beierle et al., “Cryptanalysis of the GPRS Encryption Algorithms GEA-1 and GEA-2. EUROCRYPT 2021,“ *Advances in Cryptology - EUROCRYPT 2021 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Zagreb, Croatia, pp. 155-183, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[38] Karsten Nohl, and Luca Melette, GPRS Intercept: Wardriving your country, Chaos Communication Camp, 2011. [Google Scholar] [Publisher Link]

[39] Lee Dryburgh, and Jeff Hewett, *Signalling System, No. 7 (SS7/C7) Protocols, Architectures and Service*s, Cisco Systems Inc, Cisco Press, Indianapolis, 2005. [Google Scholar] [Publisher Link]

[40] Sergey Puzankov, “Stealthy SS7 Attacks,” *Journal of ICT Standardization*, vol. 5, no. 1, pp. 39-52, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[41] Bhanu Teja Kotte, “*Analysis and Experimental Verification of Diameter Attacks in Long Term Evolution Networks*,” M.Sc. Thesis, Aalto University, Stockholm, Sweden, 2016. [Google Scholar] [Publisher Link]

[42] Xinxin Hu et al., “Signalling Security Analysis: Is HTTP/2 Secure in 5G Core Network?,” *IEEE 10th International Conference on Wireless Communications and Signal Processing*, Hangzhou, China, pp. 1-6, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[43] Nathalie Wehbe et al., “A Security Assessment of HTTP/2 Usage in 5G Service Based Architecture,” *IEEE Communications Magazine*, vol. 61, no. 1, pp. 48-54, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[44] Altaf Shaik et al., “Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems,” *arXiv Preprint*, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[45] Jean Walrand, and Pravin Varaiya, *Wireless Networks* , High-Performance Communication Networks, 2nd Edition, Morgan Kaufmann, Elsevier Inc., 2000. [Google Scholar] [Publisher Link]

[46] R.P. Merrett, and S.J. Buttery, *Cordless Technology in a Mobile Environment*, Mobile Systems, pp. 81-96, Springer, Boston, MA, 1998. [CrossRef] [Google Scholar] [Publisher Link]

[47] Stefen Lucks et al., “Attacks on the Dect Authentication Mechanisms,” *Topics in Cryptology - The Cryptographers' Track at the RSA Conference*, San Francisco,CA, USA, pp. 48-65. 2009. [CrossRef] [Google Scholar] [Publisher Link]

[48] Erik Tews, ”*DECT Security Analysis*,” Ph.D. Thesis, Doctoral Dissertation, Technische Universität Darmstadt, 2012. [Google Scholar] [Publisher Link]

[49] International Telecommunications Union (ITU), *Handbook on Satellite Communications*, 3rd ed., John Wiley & Sons Inc, 2002. [Google Scholar]

[50] Benedikt Driessen et al., “Do Not Trust Satellite Phones: A Security Analysis of Two Satphone Standards,” *IEEE Symposium on Security and Privacy*, San Francisco, CA, USA, pp. 128-142, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[51] Kunagorn Kunavut, “An Overview of Digital Trunked Radio: Technologies and Standards,” *The Journal of Industrial Technology*, vol. 10, no. 2, pp. 111-121, 2014. [Google Scholar] [Publisher Link]

[52] Carlo Meijer, Wouter Bokslag, and Jos Wetzels, *TETRA:BURST, 2023*. [Online]. Available: https://www.cryptomuseum.com/radio/tetra/burst.htm#pub

[53] Cornelius Jenkins Riddler, Vulcan: A Proprietary Cipher of the 1970s, 2014. [Online]. Available:https://www.cryptomuseum.com/crypto/motorola/saber/files/vulcan_201409.pdf

[54] GSMA. Mobile Telecommunications Security Landscape Report, 2024. [Online]. Available: https://www.gsma.com/solutions-and impact/technologies/security /wp-content /uploads/ 2024/07/Security-Landscape-2024-Issue-intro-contents.pdf