Lightweight Cryptography as a tool to meet Singapore's Carbon Emission Targets By Ananya Kharbanda

Abstract

Cryptographic practices play a vital role in securing digital communication and financial transactions, but their energy-intensive nature poses significant environmental challenges. The increasing energy demands of cryptographic algorithms and protocols have created a growing tension between robust security measures and environmental sustainability, particularly in the context of massive data centers and emerging technologies like quantum computing and the Internet of Things (IoT). Singapore is a hub of business and trading, and therefore requires robust cryptographic systems. This paper explores various mitigation efforts, including the development of energy-efficient cryptographic algorithms, hardware acceleration, server virtualization, and the integration of renewable energy sources in data centers. It also discusses Singapore's Smart Nation initiative, focusing on the country's efforts to integrate renewable energy into its digital infrastructure, enhancing sustainability while maintaining financial and technological competitiveness. In conclusion, the study emphasizes the need for a multifaceted approach that balances security, efficiency, and sustainability in cryptographic practices, addressing pertinent environmental concerns while also meeting the needs of national security and economic growth.

Introduction

The growth (McCurley) of the internet and the increasing reliance on secure communication protocols have led to a rise in the energy consumption associated with encryption processes. The issue of energy consumption for encryption has only grown ever since it was first brought up in the early 2000s. As the tech industry begins to take its first steps to reduce its ecological impact, it becomes prudent to explore the evolution of encryption methods and their implications on climate change.

In the early stages of digital communication, encryption was primarily employed by governments and large organizations to secure sensitive information (Berret). Traditional cryptographic techniques, such as symmetric-key cryptography, were computationally less intensive, and the environmental impact was relatively modest. However, with the advent of the internet and the widespread adoption of digital communication in the late 20th century, the demand for more robust encryption to protect sensitive personal information has grown exponentially (Abdalla et al.). Common types of encrypted data that people may encounter include encrypted messages in communication apps like WhatsApp, encrypted files on cloud storage platforms such as Google Drive, and encrypted payment information during online transactions using services like PayPal or credit card portals.

One of the major changes in commonly used encryption is the shift towards public-key cryptography, particularly with the introduction of the RSA algorithm (Milanov). Public-key cryptography, while providing enhanced security, has introduced higher computational requirements. This led to an increase in the processing power and energy consumption associated with encryption practices, as complex mathematical operations became integral to securing digital communication. As internet (Wendl et al.) usage expanded globally, so did the implementation of secure communication protocols like SSL/TLS for web browsing and email (Das and Samdaria). These protocols rely on cryptographic algorithms to ensure the confidentiality and integrity of data in transit. The adoption of encryption became widespread, driven not only by security concerns but also by privacy considerations.

One of the latest large-scale developments in the internet is the rise of cloud computing. Cloud services, which host vast amounts of data for individuals and organizations, rely on encryption to protect sensitive information. The constant need for data encryption and decryption in the cloud contributes to the overall energy consumption of data centers.

While encryption is crucial for safeguarding sensitive information, it requires energy-intensive computations, contributing to the carbon footprint associated with digital technologies. This environmental impact is a growing concern as questions about climate change and sustainability have become more prominent globally (Abbass et al.). Efforts have been made to address the environmental implications of encryption practices. Researchers and technologists are exploring more energy-efficient cryptographic algorithms, optimizing existing protocols, and promoting the use of renewable energy sources in data centers (Manganelli et al.). Striking a balance between maintaining robust security measures and mitigating the environmental impact of encryption remains an ongoing challenge as society continues to grapple with the implications of digitalization on climate change.

Currently, the majority of data centers powering these computations rely on traditional energy sources, further exacerbating environmental concerns. This trend contradicts the objectives outlined in the Paris Agreement, which aims to reduce greenhouse gas emissions and limit climate change (UNFCCC). The growing energy consumption from cryptographic practices highlights the need for sustainable approaches within digital technologies. Efforts to mitigate this impact have focused on the optimization of data center operations to minimize energy usage, and the promotion of renewable energy sources like solar and wind power to power data centers. However, the development of more energy-efficient cryptographic algorithms and protocols must also be a part of these efforts. Addressing the environmental implications of cryptographic practices requires collaboration among various stakeholders, including researchers, industry leaders, and policymakers. Finding a balance between maintaining robust security measures and reducing the environmental footprint of encryption processes is crucial to aligning with the goals of the Paris Agreement and promoting sustainability in digital infrastructures.

This paper takes a deeper look at the need for more efficient and less computationally intensive cryptography for the world. Beginning with the evolution of more-intensive cryptographic standards, it will then look at trends driving the proliferation of these standards and their consequences for environmental sustainability. It will conclude with a look at some efforts to mitigate the impact of highly intensive cryptographic standards, and what the implications, opportunities and challenges these hold for the world in general and Singapore in particular.

Evolution of Cryptography (Less-Intensive to More-Intensive)

In the early stages of digital communication, cryptographic techniques were primarily focused on securing sensitive information using symmetric-key cryptography. This approach involves using a single shared key for both encryption and decryption, making it relatively less computationally intensive (Sharma et al.).

Symmetric-key cryptography, while effective for securing data, had limitations in terms of key management and secure key exchange over insecure channels. As digital communication expanded and the internet became more pervasive, the need for stronger encryption mechanisms became apparent. This led to the development and adoption of asymmetric encryption algorithms, such as the RSA algorithm and Elliptic Curve Cryptography (ECC) (Mahto and Yadav).

Public-key cryptography revolutionized the field by introducing the concept of key pairs – a public key for encryption and a private key for decryption (Yilek et al.). This approach addressed the key management challenges of symmetric-key cryptography and enabled secure key exchange protocols like Diffie-Hellman key exchange (Li).

The RSA algorithm, named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman, relies on the computational complexity of factoring large prime numbers (Thabit et al.). While RSA provided enhanced security, it also introduced higher computational requirements due to its reliance on modular exponentiation operations. This shift towards asymmetric encryption marked a milestone in the evolution of cryptography but also contributed to increased energy consumption in encryption processes.

Similarly, Elliptic Curve Cryptography (ECC) gained popularity for its ability to provide strong security with relatively smaller key sizes compared to RSA (Ullah et al.). ECC relies on mathematical properties of elliptic curves to achieve secure encryption and digital signatures. However, ECC also requires computational-intensive operations, especially in key generation and elliptic curve scalar multiplication.

As digital communication continued to evolve, cryptographic techniques evolved further to address emerging security challenges. Advanced encryption standards like AES (Advanced Encryption Standard) replaced older symmetric-key algorithms like DES (Data Encryption Standard) and Triple DES due to their stronger security properties and efficiency in hardware and software implementations (Sood and Kaur).

The transition from less-intensive symmetric-key cryptography to more-intensive asymmetric encryption and modern encryption standards reflects the growing complexity of security requirements in the digital age. While these advancements provide enhanced security, they also contribute to the overall energy consumption of cryptographic processes.However, asymmetric cryptography requires significantly greater computation than symmetric-key cryptography.

Consider a 1000 Unicode character email, approximately 2000 bytes, involves distinct computational processes and efficiencies depending on the cryptographic method employed. Encrypting it via symmetric key cryptography, which uses the same key for both encryption and decryption, is generally efficient and operates linearly with the length of the plaintext. This method involves generating a single key, encrypting each block of plaintext, and combining the encrypted blocks to form the ciphertext. AES, a widely used symmetric algorithm, supports key sizes of 128, 192, or 256 bits and encrypts data in 128-bit blocks through a series of transformation rounds. These transformations, optimized for performance, are accelerated by modern CPU instructions like AES-NI, making AES particularly suitable for encrypting large amounts of data efficiently.

In contrast, RSA, an asymmetric cryptographic algorithm, uses a pair of public and private keys generated from two large prime numbers. While RSA is highly secure, it is computationally intensive due to the resource-heavy process of modular exponentiation. This makes RSA less ideal for bulk data encryption. For a 1000-character email, using RSA to encrypt each chunk of plaintext would be inefficient compared to AES. Therefore, a practical approach involves using RSA to securely exchange an AES key, which then encrypts the email content. This combination leverages the strengths of both algorithms: the efficiency of AES for data encryption and the security of RSA for key management.

Research has explored the computational requirements and energy consumption of various cryptographic techniques, highlighting the trade-offs between security and energy efficiency (Thabit et al.) . These studies underscore the importance of balancing security needs with energy-conscious cryptographic implementations to mitigate the environmental impact of encryption practices.

Increased Adoption of Cryptographic Techniques

The increased adoption of cryptographic techniques across digital applications has been fueled by the exponential increase in digital communication and the need to protect sensitive information from unauthorized access both on specific devices and in transit (Ullah et al.; Ketha). Online communication platforms, such as messaging apps, email services, and social media portals handle vast amounts of sensitive information, including personal conversations, financial transactions, and confidential documents(Naeem) . Encryption ensures that this data remains secure and confidential, even if intercepted by malicious actors.

In fact, messaging apps like WhatsApp and Signal and email services like ProtonMail tout the privacy and security of their end-to-end encryption as a differentiator from their competitors (Rösler et al.; Kobeissi)

Cloud computing has also played a significant role in the increased adoption of encryption. With the shift towards cloud-based storage and computing services, organizations and individuals rely on encryption to protect data stored in the cloud. Encrypted files on cloud storage platforms, such as Google Drive and Dropbox, ensure that data remains confidential and inaccessible to unauthorized users (Daryabar et al.).

Furthermore, the rise of e-commerce and online payment systems has driven the adoption of encryption in financial transactions. Services like PayPal, credit card portals, and cryptocurrency exchanges use encryption protocols to secure payment information and prevent fraudulent activities (Adewole et al.).

Researchers have found a significant correlation between the volume of encrypted data and the energy-intensive computations required for encryption and decryption (Zhou et al.). In the context of Singapore, a vast amount of data flows into and out of the country due to its status as a major global financial hub and data center destination; Singapore is home to 100 data centers, 1,195 cloud service providers, and 22 network fabrics (Interesse).

A typical server farm processing similar volumes of data would employ a combination of symmetric key encryption for bulk data and asymmetric encryption for key exchanges. Advanced Encryption Standard (AES) can encrypt data at a rate of approximately 1 gigabyte per second using hardware acceleration (AES-NI) on modern processors (Intel, 2021). Encrypting 1 petabyte (1 million gigabytes) of data, therefore, would require around 1 million processor seconds, or approximately 278 processor hours, assuming continuous operation.

The energy consumption of such operations is considerable. A study by the U.S. Department of Energy's Lawrence Berkeley National Laboratory reported that data centers in the United States consumed about 70 billion kWh in 2014, with significant portions attributed to computational tasks, including encryption. Given Singapore's efforts towards energy efficiency, with data centers consuming an estimated 7% of the country's total electricity in 2020, the energy demands for encrypting large data volumes remain substantial.

Comparatively, large-scale data centers like Google's, which manage extensive data volumes, consumed about 12.4 terawatt-hours (12.4 billion kWh) of energy globally in 2020 (Google, 2021). The energy demands for cryptographic operations highlight the need for optimization in encryption technologies and infrastructure to mitigate the substantial energy impacts. This is particularly crucial in data-heavy environments like Singapore, where data centers are pivotal to the digital economy.

These examples underscore the importance of continuing innovation in cryptographic processes and data center efficiency to manage the energy implications of securing large-scale data flows.

As the demand for encryption continues to grow with increased digitalization, finding energy-efficient cryptographic solutions becomes imperative to mitigate their environmental impact (Kohli et al.).

Tension Between Security and Sustainability

Cryptographic practices face a fundamental tension between maintaining robust security measures and minimizing environmental impact. Encryption is crucial for safeguarding sensitive information, but the algorithms and protocols that enable strong encryption often require significant computational resources, leading to increased energy consumption and carbon emissions. This challenge becomes even more pronounced with the advent of quantum computing, which threatens to break long-established cryptographic methods, necessitating a transition to quantum-resistant systems. However, this transition is complex and requires careful consideration of both security and sustainability.

The rise of the Internet of Things (IoT) amplifies this tension, as the demand for lightweight cryptography that can withstand quantum computing attacks increases. This situation raises critical questions about how users will adapt to quantum technology and its impact on mobile internet security, a key aspect of modern cybersecurity.

To address these challenges, the deployment of post-quantum cryptographic techniques and privacy-enhancing technologies is essential. These solutions are crucial for future security, especially in light of evolving regulations and the growing data collection by IoT devices.

In conclusion, the tension between security and sustainability in cryptographic practices requires a comprehensive approach that balances the need for robust security with the environmental impacts of encryption, while also preparing for the challenges posed by quantum computing.

Mitigation efforts

Cryptographic operations are fundamental to securing digital communication and transactions, yet their energy-intensive nature raises environmental concerns. Mitigation efforts encompass various strategies aimed at reducing the environmental footprint while maintaining security and operational efficiency (Abdullah and Lim).

Efforts to develop energy-efficient cryptographic algorithms are underway, focusing on reducing computational requirements without compromising security. The NIST Lightweight Cryptography Standardization Process has led to the adoption of algorithms like Simon and Speck, designed for resource-constrained environments such as IoT devices (Gookyi et al.; Hou et al.). These algorithms prioritize minimal energy consumption while maintaining robust security measures, making them suitable for energy-efficient cryptographic operations.

Algorithmic optimizations play a crucial role in enhancing energy efficiency. Techniques such as algorithmic pruning, where redundant computations are minimized, and parallel execution of cryptographic tasks on multicore processors, contribute to reduced energy consumption. Additionally, hardware acceleration, such as specialized cryptographic coprocessors, further improves energy efficiency by offloading cryptographic computations from general-purpose processors (Carreira-Perpinán and Idelbayev; Nagendra and Sekhar; Busby et al.). Singapore is embracing the use of energy-efficient cryptographic algorithms to minimize computational overhead while maintaining robust security (Sharon). This is particularly crucial for the financial sector, where high-frequency and algorithmic trading demand substantial computational resources. Optimizing these algorithms reduces energy consumption and enhances the overall efficiency of financial transactions.

Sustainable practices encompass a holistic approach that integrates energy efficiency, environmental responsibility, and long-term sustainability goals. Energy-efficient protocols, such as Transport Layer Security (TLS) and Secure Shell (SSH), are critical components of cryptographic operations. Efforts to optimize these protocols for energy efficiency focus on reducing computational overhead and resource utilization (Sikeridis et al.). For example, Cloudflare's implementation of TLS 1.3 prioritizes minimal energy consumption in cryptographic processes while maintaining robust security measures, contributing to sustainable cryptographic practices across the internet.

Effective management of cryptographic keys and certificates is essential for optimizing resource usage and minimizing energy consumption. Automated key management systems, certificate lifecycle management tools, and key rotation strategies streamline cryptographic processes while reducing energy waste. Efficient lifecycle management practices contribute to energy savings and operational efficiency in cryptographic operations (Leng et al.).

Optimizing data center operations is another key aspect of mitigating the environmental impact of cryptographic operations. Data centers are significant consumers of energy, including in cryptographic processes (Huang et al.). Advanced cooling techniques, like free cooling and liquid immersion cooling, contribute significantly to energy efficiency in data centers. For example, Google's data centers leverage free cooling systems, where ambient air or water is used for cooling instead of traditional mechanical refrigeration, reducing energy expenditure for cooling operations (Gong et al.). Overall, by reducing the energy load, the efficiency of high energy cooling systems is enhanced.

Server virtualization is another strategy employed to reduce energy consumption in data centers (Satra et al.). By consolidating multiple virtual machines onto fewer physical servers, server virtualization reduces idle hardware and optimizes resource utilization. This consolidation not only reduces energy consumption but also simplifies management and maintenance tasks, leading to overall operational efficiency gains. Furthermore, workload optimization and load balancing techniques help distribute computational tasks evenly across data center resources, preventing resource bottlenecks and reducing energy waste. Dynamic workload management systems adjust resource allocations in real time based on demand, optimizing energy usage without compromising performance (MirhoseiniNejad et al.). Singapore’s data centers are also moving towards server virtualization and workload optimization strategies to improve resource utilization and reduce energy waste.

The integration of renewable energy sources into data centers is a pivotal step towards sustainable cryptographic practices. Renewable energy, including solar, wind, hydroelectric, and geothermal power, offers a clean and sustainable alternative to fossil fuel-based electricity generation, significantly reducing the carbon footprint of data centers and cryptographic operations (Rahman et al.). Major technology companies have made substantial commitments to renewable energy integration in their data centers. For instance, Microsoft's Azure data centers are powered by 100% renewable energy, with investments in solar and wind projects to offset energy consumption (Acun et al.). By sourcing renewable energy certificates and engaging in power purchase agreements (PPAs) for renewable energy, Microsoft ensures that its data center operations are environmentally responsible (Hundt et al.). This shift not only reduces the carbon footprint of data centers but also supports Singapore's aim to become a green technology leader. Similarly, Amazon Web Services (AWS) has launched renewable energy projects globally, including wind and solar farms, to power its data centers sustainably (Xu et al.). AWS's commitment to achieving net-zero carbon emissions includes renewable energy integration in cryptographic operations, contributing to overall sustainability goals.

These case studies highlight the tangible operational efficiencies that result from adopting sustainable practices in cryptographic operations. By leveraging energy-efficient algorithms, optimizing data center operations, integrating renewable energy sources, and adhering to regulatory standards, organizations can further mitigate the environmental impact of cryptographic processes while ensuring robust security and operational reliability.

The adoption of green data center principles promotes sustainability in cryptographic operations by integrating energy-efficient infrastructure design, renewable energy sources, and waste heat reuse. Green data center initiatives aim to maximize resource utilization, minimize energy waste, and reduce carbon emissions in cryptographic processes. Collaborative efforts between data center operators, environmental organizations, and regulatory bodies drive the adoption of sustainable practices in data center operations, benefiting cryptographic activities as well.

The approaches of these global giants align with Singapore’s initiatives to integrate renewable energy and mitigate the environmental impact of industrial processes. Major technology companies in Singapore are committing to sourcing their energy from renewable sources.

In conclusion, mitigating the environmental impact of cryptographic operations requires a multifaceted approach that integrates energy-efficient algorithms, data center optimizations, renewable energy integration, sustainable practices, and regulatory compliance. Industry initiatives, case studies, and technological advancements demonstrate the feasibility of achieving energy-efficient and environmentally responsible cryptographic operations. By prioritizing sustainability in cryptographic practices, organizations can reduce their carbon footprint, contribute to environmental conservation, and align with global efforts towards a greener future.

Efficient cryptography and the Singapore Smart Nation Initiative

The integration of renewable energy into data center operations in Singapore is a strategic move that aligns with the nation's ambition to be a global financial and technological hub. Beyond carbon reduction, this shift enhances the resilience and sustainability of the country's digital infrastructure, reducing reliance on fossil fuels, improving energy security, and supporting community development through local job creation. These efforts are in line with Singapore's Smart Nation initiative, which aims to leverage advanced technologies to drive economic growth and improve the quality of life for its citizens.

Singapore’s commitment to renewable energy integration positions it as an economic and environmental leader, attracting global financial institutions and tech companies drawn by the city's dedication to sustainability and innovation. This influx of companies would bolster Singapore's GDP and strengthen its reputation as a pioneer in green technology. The transition to renewable energy is expected to spur significant advancements in green technologies within Singapore, including cutting-edge cooling systems, energy-efficient cryptographic algorithms, and urban-specific renewable energy solutions. These innovations could be commercialized and exported, establishing Singapore as a key player in the global green tech market.

As Singapore integrates renewable energy into data centers, the government is likely to implement progressive policies to encourage energy-efficient practices. These could include tax incentives, grants for green tech development, and stringent environmental standards, promoting sustainability and setting a global benchmark. This shift towards sustainable data centers will also necessitate a workforce skilled in both IT and renewable energy technologies, prompting Singapore's educational institutions to offer specialized programs in green technology and sustainable computing.

In the financial sector, the efficient and secure operation of cryptographic algorithms is crucial for supporting trading activities, which are vital to Singapore's economy. The energy demands of data centers hosting financial platforms and trading algorithms are substantial, reflecting the critical role of digital technologies in financial transactions. A deeper analysis could quantify the proportion of Singapore's GDP attributable to financial services and trading activities reliant on data centers and cryptographic algorithms, highlighting the energy intensity of these sectors and their implications for Singapore's energy landscape.

The growth of internet-based trading platforms further amplifies the demand for energy-efficient cryptographic solutions, as the energy footprint of these operations becomes more pronounced. Singapore's strategic focus on integrating renewable energy into data center operations supports the country's Smart Nation vision, enhancing its resilience, attracting global investments, and setting new standards for green technology. This proactive approach contributes to sustainable economic growth, technological advancement, and the global transition towards a more sustainable and resilient future.

Works Cited

Abbass, Kashif, et al. “A Review of the Global Climate Change Impacts, Adaptation, and Sustainable Mitigation Measures.” *Environmental Science and Pollution Research*, vol. 29, no. 28, 2022, pp. 42539–59.

Abdalla, Michel, et al. “Robust Encryption.” *Journal of Cryptology*, vol. 31, no. 2, 2018, pp. 307–50.

Abdullah, Nurul, and Amirah Lim. “The Incorporating Sustainable and Green IT Practices in Modern IT Service Operations for an Environmentally Conscious Future.” *Journal of Sustainable Technologies and Infrastructure Planning*, vol. 7, no. 3, 2023, pp. 17–47.

Acun, Bilge, et al. “Carbon Explorer: A Holistic Framework for Designing Carbon Aware Datacenters.” *Proceedings of the 28th ACM International Conference on Architectural Support for Programming Languages and Operating Systems, Volume 2*, 2023, pp. 118–32.

Adewole, Kayode, et al. “Application of Cryptocurrencies Using Blockchain for E-Commerce Online Payment.” *Blockchain for Cybersecurity and Privacy*, CRC Press, 2020, pp. 263–305.

Berret, Charles. *The Cultural Contradictions of Cryptography*. 2019. Columbia University, PhD Thesis.

Busby, James A., et al. "The IBM 4769 Cryptographic Coprocessor." *IBM Journal of Research and Development*, vol. 64, no. 5/6, 2020, pp. 3–1.

Carreira-Perpinán, Miguel A., and Yerlan Idelbayev. "'Learning-Compression' Algorithms for Neural Net Pruning." *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2018, pp. 8532–41.

Daryabar, Farid, et al. "Forensic Investigation of OneDrive, Box, GoogleDrive and Dropbox Applications on Android and iOS Devices." *Australian Journal of Forensic Sciences*, vol. 48, no. 6, 2016, pp. 615–42.

Das, Manik Lal, and Navkar Samdaria. "On the Security of SSL/TLS-Enabled Applications." *Applied Computing and Informatics*, vol. 10, no. 1–2, 2014, pp. 68–81.

Gong, Yuexuan, et al. "Advancements on Mechanically Driven Two-Phase Cooling Loop Systems for Data Center Free Cooling." *International Journal of Refrigeration*, vol. 138, 2022, pp. 84–96.

Gookyi, Dennis Agyemanh Nana, et al. "NIST Lightweight Cryptography Standardization Process: Classification of Second Round Candidates, Open Challenges, and Recommendations." *Journal of Information Processing Systems*, vol. 17, no. 2, 2021, pp. 253–70.

Hou, ZeZhou, et al. "Improve Neural Distinguishers of Simon and Speck." *Security and Communication Networks*, vol. 2021, no. 1, 2021, p. 9288229.

Huang, Pei, et al. "A Review of Data Centers as Prosumers in District Energy Systems: Renewable Energy Integration and Waste Heat Reuse for District Heating." *Applied Energy*, vol. 258, 2020, p. 114109.

Hundt, Steffen, et al. "Power Purchase Agreements and Financing Renewables: An Interdependency." *Journal of Structured Finance*, vol. 27, no. 1, 2021, pp. 35–50.

Interesse, Giulia. *Singapore's Data Center Sector: Regulations, Incentives, and Investment Prospects*. 1 Sept. 2023, https://www.aseanbriefing.com/news/singapores-data-center-sector-regulations-incentives-and-investment-prospects/.

Ketha, Anirudh. "The Evolution of Cryptography and a Contextual Analysis of the Major Modern Schemes." *NHSJS Reports*, 2024.

Kobeissi, Nadim. "An Analysis of the Protonmail Cryptographic Architecture." *Cryptology ePrint Archive*, 2018.

Kohli, Varun, et al. "An Analysis of Energy Consumption and Carbon Footprints of Cryptocurrencies and Possible Solutions." *Digital Communications and Networks*, vol. 9, no. 1, 2023, pp. 79–89.

Leng, Jiewu, et al. "Blockchain-Empowered Sustainable Manufacturing and Product Lifecycle Management in Industry 4.0: A Survey." *Renewable and Sustainable Energy Reviews*, vol. 132, 2020, p. 110112.

Li, Nan. “Research on Diffie-Hellman Key Exchange Protocol.” *2010 2nd International Conference on Computer Engineering and Technology*, vol. 4, 2010, pp. V4-634-V4-637, https://doi.org/10.1109/ICCET.2010.5485276.

Mahto, Dindayal, and Dilip Kumar Yadav. “Performance Analysis of RSA and Elliptic Curve Cryptography.” *Int. J. Netw. Secur.*, vol. 20, no. 4, 2018, pp. 625–35.

Manganelli, Matteo, et al. “Strategies for Improving the Sustainability of Data Centers via Energy Mix, Energy Conservation, and Circular Energy.” *Sustainability*, vol. 13, no. 11, 2021, p. 6114.

McCurley, Kevin S. “Cryptography and the Internet: Lessons and Challenges.” *Advances in Cryptology — ASIACRYPT ’96*, edited by Kwangjo Kim and Tsutomu Matsumoto, Springer Berlin Heidelberg, 1996, pp. 50–56.

Milanov, Evgeny. “The RSA Algorithm.” *RSA Laboratories*, 2009, pp. 1–11.

MirhoseiniNejad, SeyedMorteza, et al. “Joint Data Center Cooling and Workload Management: A Thermal-Aware Approach.” *Future Generation Computer Systems*, vol. 104, 2020, pp. 174–86.

Naeem, Samreen. “Network Security and Cryptography Challenges and Trends on Recent Technologies.” *Journal of Applied and Emerging Sciences*, vol. 13, no. 1, 2023, pp. 01–08.

Nagendra, M., and M. Chandra Sekhar. “Performance Improvement of Advanced Encryption Algorithm Using Parallel Computation.” *International Journal of Software Engineering and Its Applications*, vol. 8, no. 2, 2014, pp. 287–96.

Rahman, Abidur, et al. “Environmental Impact of Renewable Energy Source Based Electrical Power Plants: Solar, Wind, Hydroelectric, Biomass, Geothermal, Tidal, Ocean, and Osmotic.” *Renewable and Sustainable Energy Reviews*, vol. 161, 2022, p. 112279.

Rösler, Paul, et al. “More Is Less: On the End-to-End Security of Group Chats in Signal, Whatsapp, and Threema.” *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, IEEE, 2018, pp. 415–29.

Satra, Ramdan, et al. “Comparison of Server Technologies Using Kernel-Based Virtual Machine and Container Virtualization.” *AIP Conference Proceedings*, vol. 2595, no. 1, AIP Publishing, 2023.

Sharma, Sonali, et al. “A Study of Post Quantum Cryptographic Security Model Using Symmetric Key Algorithm.” *International Journal of Intelligent Systems and Applications in Engineering*, vol. 11, no. 5s, Apr. 2023, pp. 181–98.

Sharon, Alita. “Singapore: AI and Quantum Transforming Financial Services.” *OpenGov*, 9 July 2024, https://opengovasia.com/2024/07/09/singapore-ai-and-quantum-transforming-financial-services/.

Sikeridis, Dimitrios, et al. “Assessing the Overhead of Post-Quantum Cryptography in TLS 1.3 and SSH.” *Proceedings of the 16th International Conference on Emerging Networking EXperiments and Technologies*, 2020, pp. 149–56.

Sood, Roopali, and Harpreet Kaur. “A Literature Review on Rsa, Des and Aes Encryption Algorithms.” *Emerging Trends in Engineering and Management*, 2023, pp. 57–63.

Thabit, Fursan, et al. “Data Security Techniques in Cloud Computing Based on Machine Learning Algorithms and Cryptographic Algorithms: Lightweight Algorithms and Genetics Algorithms.” *Concurrency and Computation: Practice and Experience*, vol. 35, no. 21, 2023, p. e7691.

Ullah, Shamsher, et al. “Elliptic Curve Cryptography; Applications, Challenges, Recent Advances, and Future Trends: A Comprehensive Survey.” *Computer Science Review*, vol. 47, 2023, p. 100530.

UNFCCC, United Nations Framework Convention on Climate Change. *The Paris Agreement*. https://unfccc.int/process-and-meetings/the-paris-agreement.

Wendl, Moritz, et al. “The Environmental Impact of Cryptocurrencies Using Proof of Work and Proof of Stake Consensus Algorithms: A Systematic Review.” *Journal of Environmental Management*, vol. 326, no. Pt A, Jan. 2023, p. 116530, https://doi.org/10.1016/j.jenvman.2022.116530.

Xu, Minxian, et al. “A Self-Adaptive Approach for Managing Applications and Harnessing Renewable Energy for Sustainable Cloud Computing.” *IEEE Transactions on Sustainable Computing*, vol. 6, no. 4, 2020, pp. 544–58.

Yilek, Scott, et al. “When Private Keys Are Public: Results from the 2008 Debian OpenSSL Vulnerability.” *Proceedings of the 9th ACM SIGCOMM Conference on Internet Measurement*, 2009, pp. 15–27.

Zhou, Boyou, et al. “High-Performance Low-Energy Implementation of Cryptographic Algorithms on a Programmable SoC for IoT Devices.” *2017 IEEE High Performance Extreme Computing Conference (HPEC)*, IEEE, 2017, pp. 1–6.