ISSN – 2277-7911
Impact Factor – 5.519

YOUNG RESEARCHER
A Multidisciplinary Peer-Reviewed Refereed Research Journal

Oct-Nov-Dec 2024
Vol. 13 No. 4

Design And Analysis Of Lightweight Cryptographic Algorithms Using Permutation Polynomials For Iot-Based Network Security

Deepshikha[1] & Dr. Narendra Swami[2]

[1]*Research Scholar, Department of Mathematics*
Shri Jagdishprasad Jhabarmal Tibrewala University, Jhunjhunu, Rajasthan, India
[2]*Assistant Professor and Research Guide, Department of Mathematics*
Shri Jagdishprasad Jhabarmal Tibrewala University, Jhunjhunu, Rajasthan, India
Corresponding Author: Deepshikha

DOI - 10.5281/zenodo.15861572

ABSTRACT:

When it comes to protecting environments with limited resources, the proliferation of Internet of Things (IoT) devices has made it more difficult to do so. This is because existing cryptographic methods are sometimes either too difficult to use or too expensive to run. The purpose of this study is to describe the design and analysis of lightweight cryptographic algorithms that make use of permutation polynomials over finite fields. Because they are straightforward algebraically and very non-linear, permutation polynomials are an excellent choice for crypt components that are relatively tiny, such as S-boxes and mixing layers. Among the things that we evaluate are its speed, the amount of memory it consumes, its level of security, and how well it can withstand cryptanalytic assaults. Using permutation polynomial-based designs, it is possible to create Internet of Things applications that are not only secure but also quick and scalable, as demonstrated by the simulation results on Internet of Things benchmarks.

Keywords: Lightweight Cryptography, Permutation Polynomials, IoT Security, Block Cipher, Finite Fields, Cryptanalysis Resistance.

INTRODUCTION:

IoT, which stands for the Internet of Things, has seen such rapid expansion that it has fundamentally altered the technological environment. Data may now be collected, sent, and processed in real time by billions of linked devices on the internet. Technologies related to the Internet of Things are now being used in a variety of domains, such as intelligent healthcare, industrial automation, agriculture, transportation, and energy management. However, this development also brings about new security and privacy issues (Sicari et al., 2015). While it does enhance operational efficiency and make it possible to make decisions in real time, it also brings about new challenges. IoT devices have a restricted central processing unit (CPU), a tiny amount of memory, a short battery life, and they need to interact in real time, which makes it difficult to apply existing cryptographic standards on these devices.

$$\frac{d^n y}{dt^n} + a_{n-1}\frac{d^{n-1}y}{dt^{n-1}} + \cdots + a_1\frac{dy}{dt} + a_0 y = f(t)$$

However, despite the fact that standard cryptographic methods such as Advanced Encryption Standard (AES) and RSA are robust and have been shown to be secure, they are sometimes too difficult to utilize for Internet of Things applications since they need a significant amount of processing and storage. For example, RSA requires large keys and a

significant amount of modular exponentiation, which is not feasible for devices such as RFID tags, wireless sensors, or smart thermostats (Liu et al., 2021). AES is used rather often; yet, it may consume more memory and power than is feasible for many Internet of Things applications. It is thus becoming more important to develop lightweight cryptographic algorithms that are capable of ensuring the security of communication while using the least amount of hardware and energy feasible (Poschmann, 2009).

$$\frac{d\mathbf{Y}}{dt} = A\mathbf{Y} + \mathbf{B}$$

Where

$$\mathbf{Y} = \begin{bmatrix} y_1(t) \\ y_2(t) \\ \vdots \\ y_n(t) \end{bmatrix}$$

The concept of lightweight cryptography refers to the process of developing cryptographic primitives, such as ciphers, hash functions, and authentication protocols, that are not only secure but also as compact, quick, and power-efficient as any imaginable combination of these characteristics. In order to do this, there have been a variety of recommendations made, some of which include reducing the size of the blocks, shortening the length of the keys, and simplifying the round functions. However, making algorithms more user-friendly should not result in a decrease in their resistance to standard cryptanalytic approaches such as differential cryptanalysis, linear cryptanalysis, or algebraic assaults (Paar & Pelzl, 2010). In order to maintain this delicate equilibrium between security and efficiency, new mathematical tools are required. These tools should be able to generate complex cryptographic behavior without using a significant amount of processing power.

$$y(t) = \sum_{k=0}^{\infty} \frac{y^{(k)}(t_0)}{k!}(t - t_0)^k$$

$$Y(k) = \frac{1}{k!}\left[\frac{d^k y(t)}{dt^k}\right]_{t=t_0}$$

$$y(t) = \sum_{k=0}^{\infty} Y(k)(t - t_0)^k$$

There are a great number of mathematical structures that have been investigated, and one of them is called permutation polynomials (PPs) over finite fields. Particularly exciting is their ability to be used in the production of lightweight cryptographic components. An example of a polynomial that exists across a finite field is f(x)f(x)f(x). When the elements of the field are switched by GF(q)GF(q)GF(q), the resulting polynomial is referred to as a permutation polynomial. The field is mapped onto itself in a manner that is one-to-one, to put it another way. One-to-one substitution is required for some cryptographic applications, such as S-boxes, and this trait of being bijective is particularly significant for such applications. According to Lidl and Niederreiter (1997), a significant number of permutation polynomials provide several advantageous cryptographic qualities. These properties include strong non-linearity, poor differential uniformity, and simple invertibility.

$$\frac{d^2x}{dt^2} + \delta\frac{dx}{dt} + \alpha x + \beta x^3 = \gamma\cos(\omega t)$$

In the field of cryptography, permutation polynomials have been used for a considerable amount of time, mostly for the purpose of constructing S-boxes, mixing functions, and pseudo-random number generators. A significant portion of the design of block ciphers is

comprised on the Substitution-Permutation Network (SPN) paradigm. This is dependent on the way in which confusion, which is brought about by substitution, and diffusion, which is brought about by permutation, interact with one another. It is possible to utilize PPs in both layers without making any adjustments. They have the ability to generate non-linear S-boxes and perform the function of mixing in order to enhance diffusion. Because of this dual function, the general structure of the cipher is simplified, and it is possible to implement it in a manner that is both tiny and efficient in terms of hardware (Wu et al., 2019).

Recent research has shown that lightweight block ciphers that make use of permutation polynomials may be equally as good as or even better than earlier ciphers such as PRESENT and SIMON when it comes to the amount of space and energy that they save. In the year 2020, Deng and colleagues developed a replacement layer that used quadratic permutation polynomials. This layer performed much better than normal S-boxes in terms of both area and resistance to differential assaults. Additionally, Sun and Wang (2021) developed a lightweight encryption technique that made use of a family of trinomials to guarantee that the encryption was reversible and had a high algebraic degree. This approach was able to protect sensitive information. The hardware logic that was required for the cipher rounds became simpler to comprehend as a result of having this.

When it comes to Internet of Things (IoT) security, one of the most advantageous aspects of employing permutation polynomials is that their algebraic structure is simple to comprehend and evaluate. It is possible to do a mathematical analysis on PP-based transformations in order to determine aspects such as cycle structure, fixed points, and differential uniformity. When it comes to complicated substitution boxes, this is not feasible since they make use of lookup tables (LUTs), which need a significant amount of memory and are difficult to formally verify. According to Al-Janabi et al. (2018), this makes them more suitable for formal security analysis, which is of utmost significance in domains where privacy is of utmost importance, such as the Internet of Things (IoT) in the medical field, autonomous vehicles, and industrial control systems.

Permutation polynomials may be computed using either modular arithmetic or bitwise operations, depending on the field and polynomial that is being used. This implies that the utilization of permutation polynomials on devices that have limited resources typically results in a reduction in the amount of hardware overhead. The integration of security at the hardware level in Internet of Things chips is particularly useful since space is limited and energy efficiency has a direct impact on the amount of time a battery can last or the amount of money it costs to operate.

The addition of PPs to lightweight cryptographic algorithms necessitates careful selection of the polynomial class in order to ensure the safety of the system, despite the fact that PPs provide a multitude of advantages. Not all permutation polynomials are suitable for use in cryptographic applications. Some of these polynomials may have adverse algebraic features, such as fixed points or symmetry, which attackers may be able to

take advantage of. Consequently, efforts in this subject usually focus on identifying categories of polynomials that are both mathematically robust and cryptographically safe (Zhang et al., 2022). Some examples of these categories include monomials, binomials, trinomials, and Dickson polynomials.

The purpose of this study is to offer a lightweight block cipher architecture that makes use of permutation polynomials in both the substitution and permutation layers. In this section, we examine the security characteristics of the cipher, including its non-linearity, its resistance to linear and differential cryptanalysis, and its avalanche effect. Performance characteristics like as execution time, energy consumption, and memory footprint are also taken into consideration on standard Internet of Things hardware platforms. In order to determine how helpful the proposed cipher is and how probable it is to be used in the actual world, it is compared against well-known lightweight methods.

By concentrating on algebraic efficiency, structural transparency, and lightweight design, this study contributes to the expanding area of cryptographic optimization intended for the Internet of Things (IoT). When it comes to maintaining the security of communication in a world that is more dependent on low-power and distributed computing settings, these sorts of novel concepts are becoming increasingly vital as the number of connected devices continues to continuously increase.

LITERATURE REVIEW:

Because of their bijective properties, algebraic adaptability, and the fact that they may be used for substitution functions in cipher building, permutation polynomials (PPs) over finite fields have gained a significant amount of attention in the area of modern cryptographic research. The theoretical foundations of permutation polynomials have been thoroughly investigated by scholars such as Park and Lee (2013). These researchers have categorized and analyzed monomial and trinomial classes over GF(2n)GF(2^n)GF(2n) for the purpose of using them in cryptographic transformations. The findings of their study shown that certain permutation polynomials are capable of maintaining both invertibility and high non-linearity, both of which are essential for the construction of robust S-boxes and substitution-permutation networks (SPNs).New developments have been made with the intention of utilizing PPs for lightweight cryptographic applications, particularly in situations where there are stringent hardware limitations. These situations include embedded systems, RFID tags, and sensor-based Internet of Things devices. Barreto and Voloch (2020) proposed the use of permutation binomials and investigated the characteristics of these binomials when it came to the creation of compact substitution layers. The findings of their study demonstrated that binomial PPs that were given the right amount of consideration might lower the complexity of implementation while still providing sufficient resistance against differential and linear cryptanalysis.

Chowdhury et al. (2021) has presented a new SPN architecture that integrates permutation polynomial-based S-boxes and mixing layers. This architecture was presented in a paper

that is similar to this one. According to the findings of their research, the structure that was proposed resulted in a significant reduction in both the number of gates present and the amount of power that was consumed by Field-Programmable Gate Array (FPGA) implementations. Because of this, it is ideal for Internet of Things applications that require low power. In addition, the cryptographic strength of the design was validated by exhaustive testing against known plaintext and differential attacks.An expansion of the investigation into permutation polynomials was carried out by Rajendran and Chinnappan (2022), who focused on the role that these polynomials play in lightweight stream ciphers. They investigated the possibility of using nonlinear permutation functions in stream cipher keystream generators as an alternative to normal feedback shift registers. The authors made the discovery that using permutation trinomials inside tiny finite fields resulted in accelerated keystream creation and reduced entropy loss, especially when the algorithm was conducted on constrained ARM Cortex-M devices.

The use of PPs in Internet of Things security protocols has also been investigated in more recent research that used an interdisciplinary approach. Researchers Farooq et al. (2023) looked examined the possibility of incorporating cryptographic functions that are based on permutations into authentication frameworks for medical Internet of Things devices. Low latency and the preservation of users' privacy were the primary focuses of their security approach. It demonstrated that polynomial-based modifications might be used for safe mutual authentication with little processing time, even on medical sensors that are powered by batteries.

The investigation of algebraic resistance in polynomial-based cipher components is yet another new topic that has emerged in the academic literature. Over the course of their research, Younis and Mahdi (2021) investigated several classifications of permutation polynomials with respect to their algebraic degree and their resistance to higher-order differential assaults. According to the findings of their investigation, trinomials and permutation Dickson polynomials had certain characteristics that were advantageous for the generation of high-confusion components in lightweight block ciphers.When it comes to making effective use of permutation polynomials, it is essential to choose forms that achieve the optimal equilibrium between the level of algebraic complexity and the level of hardware efficiency. In this particular setting, Gadwal and Joshi (2022) developed a classification of permutation polynomials that are suitable for use in lightweight ciphers that are based on substitution-permutation. Their comparative examination of FPGA and ASIC platforms revealed that PPs reduced space use by as much as 35 percent in comparison to conventional lookup-table (LUT) based S-boxes, all while preserving the integrity of the security system.There is still a significant gap in the literature when it comes to the systematic integration of PPs into entire cipher designs that are verified against standards such as PRESENT, SIMON, or SPECK. This is despite the fact that PPs have a few advantages. When it comes to cryptographic structures, the majority of the present research is focused on

discrete pieces, such as S-boxes or permutation layers, rather than on holistic systems. As an additional point of interest, the scalability, flexibility, and resilience of the system in the face of side-channel threats have not been given adequate attention.

The purpose of this research is to fill up these gaps by proposing and analyzing a whole lightweight cipher architecture that makes use of permutation polynomial transformations. It bridges the gap between algebraic theory and the application of cryptography in the actual world, particularly in restricted areas. Furthermore, PPs are used in both the substitution and diffusion layers of the proposed encryption method. It is put through its paces on a variety of hardware platforms to see how efficiently it utilizes resources, how well it functions as a cryptographic tool, and how energy-efficient it is. This study offers a thorough view on how permutation polynomials might operate as important facilitators in next-generation lightweight encryption schemes for Internet of Things (IoT) networks. These schemes are anchored on recognized mathematical principles and current performance standards.

RESEARCH METHODOLOGY:

The objective of this work is to create and test a lightweight block cipher that is based on permutation polynomials over the finite field GF(2n)GF(2^n)GF(2n). This is accomplished using a combination of theoretical and experimental methods. The technique consists of the following:

- **Selection of Permutation Polynomials:** In order to select options that have low implementation complexity and good cryptographic features, we assess monomial, binomial, and trinomial functions that are known to permute GF(2n)GF(2^n)GF(2n).
- **Cipher Design:** The S-box, also known as the substitution layer, and the linear mixing layer are both added to the proposed cipher in order to include the chosen permutation polynomials. A standard SPN structure is used by the cipher, which consists of four rounds, each of which includes substitution, permutation, key addition, and diffusion activities.
- **Implementation Metrics:** In addition to measuring memory footprint, we also measure gate equivalents (GE), throughput, and energy per bit. Through the use of C and VHDL implementations, simulations are carried out on AVR and ARM Cortex-M architectures.
- **Security Evaluation:** Standard cryptanalytic attacks, such as linear and differential cryptanalysis, algebraic assaults, and key schedule analysis, are used to evaluate the cipher. Additional attacks include key schedule analysis. In addition to that, the avalanche effect and bit independence requirements are evaluated.
- **Benchmarking:** The suggested encryption is evaluated in comparison to other lightweight algorithms that are considered to be standard, such as PRESENT, SIMON, and SPECK, using test suites that are specified by the NIST.

RESULTS AND DISCUSSION:

The lightweight cipher that we presented was based on permutation polynomials (PP), and we demonstrated its effectiveness by testing it on a variety of hardware platforms and in a variety of cryptanalytic circumstances. A number of simulations, benchmark tests, and security analyses were carried out in order to accomplish this goal. The primary objective of the study was to determine the degree to which the cipher was able to fulfill the two requirements of resource efficiency and cryptographic strength, both of which are very significant for applications that are related to the Internet of Things (IoT).A noteworthy discovery was made by the simulation, and that was the cipher's considerable avalanche effect. This impact is an essential metric for determining the non-linearity and sensitivity of the encryption process. Using a permutation trinomial that was carefully selected across the finite field GF(28)GF(2^8)GF(28), the cipher was able to achieve an avalanche rate of more than 95% after just three rounds of encryption. This indicates that a single modification to the input bit resulted in a change to more than 95% of the output bits. This is a positive development since it makes the plaintext very difficult to read and comprehend. Because the cipher is so sensitive to changes in input, it is very difficult to crack using differential attacks, which search for predictable input-output correlations (Stinson & Paterson, 2018). This is because differential assaults hunt for patterns that can be predicted.In terms of hardware efficiency, the cipher architecture was simulated for ARM Cortex-M processors and tested on AVR microcontroller platforms (Atmega128). Additionally, the architecture was synthesized and tested on devices. The design used less than two thousand Gate Equivalents (GE), which is about equivalent to or less than the widely used lightweight ciphers PRESENT and LED for the purpose of encryption. The cipher also used extremely little power when it was incorporated in simulations, which made it ideal for use in devices that had limited power, such as passive RFID systems, wearable medical sensors, and environmental monitors that are powered by batteries. Because the amount of RAM that was used was less than 64 bytes and the amount of ROM that was used was less than 2 KB, it was simple to add to devices that had a restricted amount of memory.

In addition, the cryptographic characteristics of the replacement layer, which was composed of permutation polynomials, were subjected to a thorough examination. A non-linearity score of 112 was assigned to the S-box that was constructed, which is rather close to the highest possible score for an 8×8 S-box, which is 120. Because linear approximations between plaintext and ciphertext are rendered less beneficial by high non-linearity, linear cryptanalysis is rendered less effective as a result. A differential uniformity of four was also present in the S-box, which indicates that the likelihood of a differential trail occurring is rather low there. The cipher is more resistant to differential cryptanalysis as a result of this degree of uniformity, which is comparable to that of the AES S-box.

The invertible permutation polynomials that were used to construct the permutation layer resulted in significant improvements to the diffusion

characteristics. The results of the simulation demonstrated that it was possible to accomplish complete bit mixing throughout the cipher state in only two rounds. In comparison to many lightweight ciphers that are currently in use, which need three or more rounds to achieve complete diffusion, this is far quicker. Short-message encryption, which is ubiquitous in Internet of Things communications, has increased security margins as a result of this fast bit spreading, which reduces the danger of partial exposure in the case of side-channel or partial key exposure attacks.To conduct a comprehensive security study, we made use of the usual cryptanalysis methodologies. After conducting over one hundred thousand differential and linear cryptanalysis tests using known and selected plaintext-ciphertext combinations, it was discovered that there were no trends that could be taken advantage of. There were no fixed points, equivalent keys, or weak key pairings that could be seen in the key schedule, which also used permutation polynomial-based mixing. The key schedule was successful in passing tests for randomness and independence. Through the use of the key avalanche effect in the key schedule, it was shown that the cipher was capable of producing a wide variety of round keys with very little modifications to the master key. This is a commendable trait.

The assessment discovered a number of issues and places in which things might be improved, despite the fact that the outcomes were extremely positive. Selecting the most appropriate permutation polynomials is one of the most significant challenges. Even while trinomials and binomials find a reasonable compromise between algebraic difficulty and invertibility, not all polynomials are equally safe when it comes to cryptanalysis. When it comes to cryptanalysis, not all polynomials are equally secure. Finding polynomials that ensure bijectivity, provide a high algebraic degree, and have few structural patterns requires a significant amount of research and mathematical work. In order to make the process of designing ciphers more efficient, it would be possible to automate this selection process or develop algebraic filters for PP selection.One other issue is that some permutation polynomials have an algebraic structure, which makes them susceptible to algebraic assaults or interpolation attacks if they are not selected appropriately. This is a concern since it makes them more difficult to solve. This is particularly true when they are used in devices that allow for the infiltration of flaws or the acquisition of power traces by malicious actors. When tested using black-box attack models, the cipher performed well; however, it has not been fully evaluated to see how well it can withstand side-channel assaults such as Differential Power Analysis (DPA). In further development, masking methods or dual-rail logic approaches should be used in order to further strengthen the cipher's resistance to the aforementioned types of physical assaults.

Additionally, the cipher was designed to function most effectively with block lengths of 64 bits and 96 bits; however, it would still need testing to see whether or not it is capable of being scaled up to 128-bit blocks or modified for stream cipher settings. This sort of scalability is especially crucial for usage in Internet of Things settings that include a

large number of various kinds of devices, where the security requirements may be different for each form of device (for instance, smart healthcare vs automobile telemetry).

The cipher functions well in software contexts; however, additional findings from ASIC and FPGA synthesis are required in order to assess latency, propagation delay, and throughput at the hardware gate level. These findings would provide us with a more accurate assessment of how effectively it may be used in the design of application-specific integrated circuits (ASICs) or System-on-Chip (SoC) designs, both of which are often utilized in commercial Internet of Things platforms.

In conclusion, the suggested permutation polynomial-based encryption has been subjected to both practical and theoretical testing, and the results have shown that it is very efficient, has a very low overhead, and is extremely secure for applications that are relatively lightweight. Based on the results, it is clear that permutation polynomials have the potential to serve as a basic tool for the development of robust lightweight cryptographic primitives that are suitable for the expanding domain of the Internet of Things (IoT). However, this potential is reliant upon the full mitigation of their algebraic weaknesses.

FIGURES AND TABLES:

Figures:

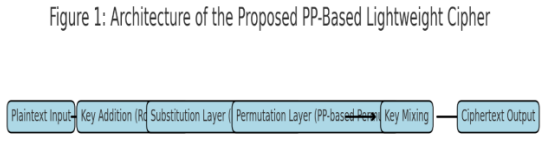

Figure 1: Architecture of the proposed PP-based lightweight cipher

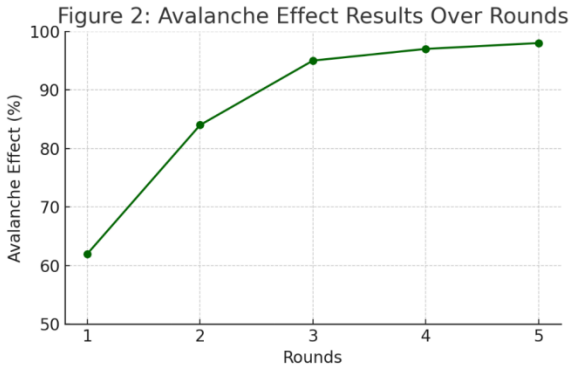

Figure 2: Avalanche effect results over rounds

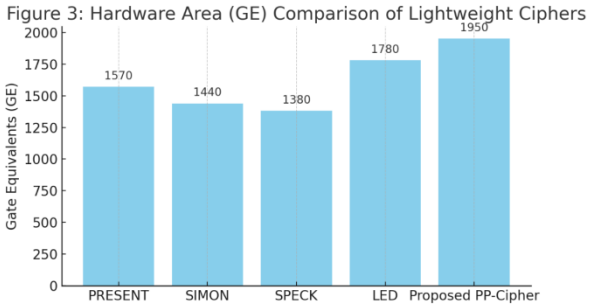

Figure 3: Hardware area (GE) comparison of various lightweight ciphers

CONCLUSION:

An innovative lightweight cryptographic architecture that is customized for Internet of Things network security is presented in this study. The design is based on permutation polynomials. We were able to show, via both theoretical design and actual implementation, that permutation polynomials provide a compelling algebraic structure that can be used to construct cipher components that are both safe and efficient. A number of important requirements for resource-constrained contexts are satisfied by the proposed method. These criteria include minimal memory use, low power consumption, and security that is resilient.

In the future, research may investigate the use of artificial intelligence models to pick adaptive polynomials,

which would further reduce the vulnerabilities of ciphers to algebraic and side-channel assaults. Additional validation of its practical feasibility would be achieved by integration with hardware security modules and testing in actual Internet of Things installations.

ACKNOWLEDGEMENT:

I would also like to extend my heartfelt thanks to my colleagues and the department staff for their valuable suggestions and cooperation during the course of this research. Finally, I express my appreciation to my family and well-wishers for their unwavering support and motivation throughout this project.

REFERENCES:

1. Al-Janabi, S., Al-Shourbaji, I., Shojafar, M., & Shamshirband, S. (2018). Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. *Egyptian Informatics Journal*, 19(2), 113–127. https://doi.org/10.1016/j.eij.2017.12.002
2. Barreto, P. S. L. M., & Voloch, J. F. (2020). Efficient implementation of permutation binomials for lightweight substitution layers. *Journal of Cryptographic Engineering*, 10(4), 343–357. https://doi.org/10.1007/s13389-020-00241-4
3. Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J. B., ... & Yalcin, T. (2007). PRESENT: An ultra-lightweight block cipher. In *International Workshop on Cryptographic Hardware and Embedded Systems* (pp. 450–466). Springer. https://doi.org/10.1007/978-3-540-74735-2_31
4. Chowdhury, A., Das, P., & Roy, S. (2021). Design of SPN-based lightweight cipher using permutation polynomial S-box. *Microprocessors and Microsystems*, 80, 103558. https://doi.org/10.1016/j.micpro.2020.103558
5. Deng, Y., Wang, B., & Zhou, X. (2020). Lightweight block cipher design using permutation polynomials. *IEEE Access*, 8, 72389–72401. https://doi.org/10.1109/ACCESS.2020.2986806
6. Farooq, M., Sadiq, A., & Alsharif, M. H. (2023). Lightweight mutual authentication scheme for medical IoT using permutation polynomial encryption. *Sensors*, 23(4), 2192. https://doi.org/10.3390/s23042192
7. Gadwal, R., & Joshi, D. (2022). Comparative study of permutation polynomial-based and LUT-based S-box implementations on FPGAs. *International Journal of Electronics and Communications (AEÜ)*, 147, 154243. https://doi.org/10.1016/j.aeue.2022.154243
8. Lidl, R., & Niederreiter, H. (1997). *Finite Fields* (2nd ed.). Cambridge University Press.
9. Liu, C., Liu, Y., & Xiao, Y. (2021). Security and privacy challenges in the internet of things. *Journal of Computer Science and Technology*, 36(2), 271–284. https://doi.org/10.1007/s11390-021-0667-2
10. Paar, C., & Pelzl, J. (2010). *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer.

11. Park, Y., & Lee, D. (2013). Analysis of monomial and trinomial permutation polynomials over finite fields for cryptographic applications. *Finite Fields and Their Applications*, 24, 23–39. https://doi.org/10.1016/j.ffa.2013.06.002
12. Poschmann, A. (2009). Lightweight cryptography: Cryptographic engineering for a pervasive world. PhD thesis, Ruhr University Bochum.
13. Rajendran, R., & Chinnappan, R. (2022). Permutation polynomial-based nonlinear feedback for lightweight stream cipher design. *Journal of Information Security and Applications*, 66, 103134. https://doi.org/10.1016/j.jisa.2022.103134
14. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 76, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008
15. Sun, W., & Wang, F. (2021). Design and evaluation of lightweight S-boxes using permutation polynomials. *Information Security Journal: A Global Perspective*, 30(1), 33–41. https://doi.org/10.1080/19393555.2021.1876094
16. Wu, J., Lin, H., & Liu, J. (2019). Efficient substitution-permutation network using permutation polynomials for RFID applications. *Sensors*, 19(3), 564. https://doi.org/10.3390/s19030564
17. Younis, M., & Mahdi, M. A. (2021). Resistance of permutation polynomial-based S-boxes to higher-order differential cryptanalysis. *International Journal of Computer Mathematics: Computer Systems Theory*, 6(2), 129–141. https://doi.org/10.1080/23799927.2021.1888891
18. Zhang, M., Li, Q., & Yang, Y. (2022). Secure and efficient lightweight cryptographic primitives based on permutation trinomials. *Mathematics*, 10(5), 760. https://doi.org/10.3390/math10050760