ISSN – 2277-7911
Impact Factor – 5.519
YOUNG RESEARCHER
A Multidisciplinary Peer-Reviewed Refereed Research Journal
Apr-May-June 2024
Vol. 13 No. 2

Secure Key Exchange Mechanisms In Public-Key Cryptography Using Permutation Polynomial-Based Transformations

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.15811332

ABSTRACT:

Secure key exchange remains a cornerstone of public-key cryptography, enabling confidential communication over unsecured channels. Traditional protocols like Diffie-Hellman and RSA rely heavily on number-theoretic assumptions. This paper proposes a novel key exchange mechanism based on permutation polynomial transformations over finite fields. These algebraically rich functions offer inherent bijectivity, high complexity, and mathematical unpredictability. The study constructs a key exchange model using permutation polynomial-based transformations and evaluates its computational feasibility, security against known attacks, and suitability for post-quantum scenarios. Initial results show promising cryptographic strength and practical efficiency. The findings suggest that permutation polynomials can be valuable tools for next-generation cryptographic protocols.

Keywords: Key Exchange, Public-Key Cryptography, Permutation Polynomials, Finite Fields, Algebraic Security, Post-Quantum Cryptography

INTRODUCTION:

Exchange of keys in a safe manner is considered to be one of the cornerstones of modern cryptography. It is possible for two or more parties to have the ability to generate a shared secret key via the usage of an insecure communication channel. This key may then be used in symmetric cryptosystems to encrypt and decode communications. When it comes to digital communication systems, such as online banking, email encryption, and Virtual Private Networks (VPNs), this basic method ensures that data is kept secret and authenticated. The security of a key exchange mechanism is dependent on its ability to withstand assaults such as man-in-the-middle, impersonation, and eavesdropping while yet preserving its viability and computing efficiency.

$$P(x) = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1 x + a_0$$

The mathematical basis for safe public-key cryptography has typically been given by conventional key exchange protocols such as the Diffie-

Hellman algorithm, which was first presented in 1976, and the RSA algorithm, which was devised in 1978. Both of these algorithms were developed in the same year. Diffie and Hellman (1976) and Rivest, Shamir, and Adleman (1978) are two examples of approaches that depend on the difficulty of certain mathematical problems. Specifically, the integer factorization issue for RSA and the discrete logarithm problem in finite fields for Diffie-Hellman are the two difficulties that are used in both techniques. There were billions of encrypted transactions all across the globe that were protected by these presumptions for many years, during which time they were almost impossible to break with conventional computer power.

$$K = P(x) \bmod 2^n$$

The advent of quantum computing, on the other hand, has raised serious concerns over the longevity of these conventional methods of cryptography. Shor's algorithm, a quantum algorithm that was developed in the 1990s, has the potential to factor big numbers and solve discrete logarithms in polynomial time if it is implemented on a quantum computer that is sufficiently powerful (Shor, 1994). This would render RSA and Diffie-Hellman unsafe. Researchers that are interested in developing cryptographic systems that are resistant to quantum assaults have developed post-quantum cryptography as a consequence of their investigation into various algebraic bases.

$$y_i = P(x_i) \text{for } i = 1,2, \dots, m$$
$$H(P(x) \mid\mid r)$$

In this light, permutation polynomials over finite fields have emerged as a potential alternative to the construction of robust cryptographic primitives. Specifically, a permutation polynomial is a kind of polynomial function that performs the function of a bijection on a finite field. It does this by mapping each element of the field to a unique output value without causing any collisions. These polynomials are particularly desirable due to the fact that they exhibit deterministic behavior, have algebraic complexity, and include inherent security characteristics. These properties include strong non-linearity, resistance to differential and algebraic assaults, and compatibility with hardware implementations (Lidl & Niederreiter, 1997). Furthermore, in contrast to typical systems that are based on big integers or elliptic curves, polynomial-based techniques may be successfully applied within constrained contexts, such as embedded systems and devices connected to the Internet of Things.

In the past, permutation polynomials have been used in the development of pseudo-random number generators, masking functions for the purpose of preventing side-channel attacks, and S-Boxes for the purpose of symmetric cryptography (Wang & Zhang, 2015; Cusick & Stanica, 2009). Despite this, they still offer a great deal of promise in the realm of key exchange protocols that has not yet been used. The algebraic properties of permutation polynomials, which make

them attractive for masking and substitution operations, also make them suitable for safe transformations in public-key exchanges for the same reason that they are desired for masking and substitution operations.

$$H = -\sum_{i=1}^{n} p_i \log_2 p_i$$

This work analyzes a unique key exchange method that is based on permutation polynomial transformations. In this mechanism, users calculate shared secrets by using their own private polynomial transformations, and then they exchange public values that are generated via polynomial evaluations. By taking advantage of the bijective and complex structure of these polynomials, the approach that has been described is able to retain computing efficiency while simultaneously defying established cryptanalytic assaults. After lattice-based or code-based post-quantum techniques, which usually have huge key sizes and extensive implementation requirements, permutation polynomial-based protocols provide a lightweight but safe alternative. These protocols provide a lightweight yet secure alternative. This works especially effectively in circumstances when there is a limited amount of memory and processing power available.

Following the establishment of the mathematical foundations and properties of permutation polynomials, a design framework for the key exchange protocol is described subsequently. Following this, an analysis is performed to determine whether or not the proposed system is secure, efficient, and resistant to both classical and quantum attacks. In the final parts, the results of the implementation, performance metrics, and a comparison with the existing public-key protocols are described.

By doing so, the purpose of this study is to give a post-quantum safe, effective, and scalable solution that is suitable for the ever-changing digital security environment. Additionally, the work aims to narrow the gap in algebraic-based key exchange systems.

LITERATURE REVIEW:

This concept of safe key exchange serves as the cornerstone around which modern cryptographic communication is built. Although the early discoveries made by Diffie and Hellman and the introduction of RSA continue to be significant milestones in cryptographic science, the development of quantum computing has significantly changed the focus of research toward alternative strategies that can withstand quantum-based threats. This is despite the fact that the introduction of RSA can be considered a significant milestone. As a result of the continued development of quantum algorithms such as Shor's and Grover's, traditional methods that are based on discrete logarithms and integer factorization are in risk of becoming outdated in the not too distant future (Chen et al., 2016).

Recent efforts have been concentrated on the investigation of algebraic cryptography, particularly systems that are based on polynomial

transformations over finite fields. Permutation polynomials have attracted a lot of attention among these due to the fact that they are difficult to solve algebraically, they have deterministic bijective mappings, and they are resistant to linear and differential assaults (Sun & Wu, 2018). Due to the fact that they allow for changes that are both safe and reversible, these mathematical structures are completely suitable for key exchange methods.

The behavior of permutation polynomials as well as their categorization have been the focus of an increasing amount of theoretical and empirical investigation. For instance, Bartoli et al. (2014) investigated exceptional polynomial classes and associated cycle patterns. These structures have a direct influence on the degree to which cryptographic mappings are unexpected. They brought attention to the significance of the permutation polynomial design in the process of generating non-linear transformations that have a high algebraic degree. Similar to this, Masuda and Kuroda (2012) examined the use of permutation trinomials in cryptography over characteristic two fields. They emphasized the lightweight nature of these trinomials, which makes them suitable for hardware systems that have limited resources.

In spite of the fact that a number of multivariate-based cryptographic primitives, such as Unbalanced Oil and Vinegar (UOV) and Hidden Field Equation (HFE) schemes, have shown that they have post-quantum potential, these primitives are frequently criticized for their high computational complexity and large key sizes (Kipnis & Shamir, 1999; Ding, 2004). As a consequence of this, permutation polynomials and other single-variable algebraic models have gained popularity. These models are able to preserve complexity without compromising efficiency, and they have grown more popular.

Not only have theoretical studies shown the effectiveness of permutation polynomial structures, but recent implementation-based research has also demonstrated that these constructs are helpful in practice. It was hypothesized by Liu et al. (2020) that an efficient implementation of a permutation polynomial-based encoding scheme over GF(2 m) was possible. Furthermore, the authors demonstrated that the system was immune to known algebraic and statistical assaults. Furthermore, the results of their studies indicate that these sorts of constructs are particularly beneficial for ensuring secure communication in real-time environments and embedded systems.

A very imaginative research was conducted by Wu and Qiao (2021), in which they presented a key encapsulation mechanism (KEM) that was based on permutation polynomial transformations. This work demonstrated that these polynomials may serve as the foundation for post-quantum cryptography protocols that are both secure and portable. Their work addressed a huge hole in public-key infrastructure by offering both theoretical security proofs and usable benchmarks. This was accomplished via the provision of both.

Although significant breakthroughs have been made, permutation polynomial-based cryptographic approaches are still not being employed to their full potential within the framework of public-key key exchange systems. With regard to symmetric key creation, replacement, or obfuscation, these structures are used in the vast majority of the systems that are currently in use. Using these mathematical foundations as a foundation, the present research endeavors to develop a key exchange protocol that is not only successful but also efficient, algebraically safe, and resistant to both classical and quantum cryptanalytic models.

RESEARCH METHODOLOGY:

Within the scope of this investigation, a key exchange protocol that is founded on permutation polynomial transformations is developed and tested via the use of a theoretical modeling and simulation-based technique.

Design Framework:

- Alice and Bob, two users, come to an agreement over a public finite field identified as GF(q)GF(q)GF(q) and a family of permutation polynomials P(x)P(x)P(x) that is known to both of them.
- Bob receives the result of Pa(b)P_a(b)Pa(b), where bbb is Bob's public input. Alice chooses a secret integer aaa, computes Pa(x)P_a(x)Pa(x), and then delivers the result to Bob.
- Bob sends back Pb(a)P_b(a)Pb(a) by following a symmetric protocol and using his own private key instead of the public key.
- The shared secret is computed by both parties using a shared function that is derived from their own secrets as well as the converted value that was received.

Evaluation Parameters:

- **Security analysis:** Resistance to man-in-the-middle, known-plaintext, and algebraic attacks.
- **Performance benchmarking:** Time complexity, key size, and memory efficiency.
- **Mathematical robustness:** Invertibility, cycle structure, and field compatibility.

Simulations were carried out using SageMath and Python's SymPy and NumPy libraries, with finite field sizes ranging from 128-bit to 256-bit domains.

RESULTS AND DISCUSSION:

Using the algebraic power of permutation polynomials over finite fields, the suggested key exchange method was able to build a mechanism for public-key communication that was both safe and efficient. With the purpose of determining whether or not this approach is suitable for use in the real world, particularly in the context of developing post-quantum cryptographic landscapes, it was subjected to stringent evaluations across a variety of domains, including security, attack resistance, performance, and mathematical robustness.

1. Security:

- **Bijectivity and Invertibility:**

The bijective characteristic of permutation polynomials serves as the foundation for one of the most important security-related aspects of our method. Every single polynomial P(x)P(x)P(x) that is selected at random from our preset family represents a one-of-a-kind invertible function over the set F2n_{2^n}F2n (Wu & Qiao, 2021). As a consequence of this, the transformation that was made to the public values cannot be reversed without the knowledge of the particular secret polynomial coefficients. This injective nature ensures that the secret key is kept confidential. Even if adversaries have access to multiple input–output samples, they are unable to derive the secret polynomial because doing so would require them to solve an overdetermined system of nonlinear equations, which is a problem that is believed to be intractable for sufficiently large nnn (Bartoli et al., 2014).

- **Hardness of Inversion:**

In the context of GF(2n2^n2n), the process of extracting the secret key may be described as solving for P(x)P(x)P(x) given a series of polynomial equations. According to Kipnis and Shamir (1999), there is no known subexponential method for solving general polynomials over large finite fields. This is a fact that has been discussed extensively in the subject of multivariate public-key cryptography. Permutation polynomials are characterized by their algebraic complexity, which makes this challenge worse. Even strong quantum techniques, such as Grover's algorithm, only give a quadratic speedup, which is inadequate to break systems with sizes more than 128 bits within the constraints of practical computing (Chen et al., 2016). Because of this, the permutation polynomials that we have chosen to use improve both the classical and quantum robustness of the system.

2. Resistance to Attacks:

- **Man-in-the-Middle (MitM) Protection:**

An element of ephemeral randomness is included into the system throughout each session. Users are responsible for generating fresh input values and polynomial "blinding" factors. A brief polynomial-derived fingerprint is sent between both parties prior to reaching an agreement on the public values. This fingerprint is produced using cryptographic hash algorithms that are applied to the polynomials. The collision-resistance of contemporary hashes makes this approach a strong deterrent against MitM attacks. Without the knowledge of the secret polynomials, MitM attackers would be unable to generate valid fingerprints, which is why this method is effective against them (Jin & Huang, 2018).

- **Algebraic Attack Resilience:**

As a result of this scheme's selection of permutation polynomials with algebraic degrees of at least seven (for example, trinomials or quartic functions), the difficulty of system-solving assaults was greatly increased. It has been shown in the research that has been conducted on multivariate cryptosystems that the complexity of

algebraic attacks increases combinatorially with increasing degrees (Patarin, 1996). As a result of selecting polynomials that possess both high degree and unpredictability in their coefficients, the implementation of algebraic factorizations or Grobner basis assaults becomes computationally difficult for field sizes ranging from 256n to 256n (Liu et al., 2020).

- **Quantum Resistance:**

In addition to the well-known performance constraints established by Shor and Grover, our method is able to take advantage of the absence of specialized quantum subalgorithms that cater to the resolution of high-degree polynomial systems. According to Bravyi and Gosset (2016), the quantum approaches that are currently available for solving equations provide very minimal advantages, in comparison to the classical complexity limitations. According to Bernstein et al. (2017), this places permutation polynomial-based key exchange among the postquantum safe protocols. This kind of key exchange demonstrates resilience not by depending on lattice hardness but rather by using structural algebraic difficulty.

3. Performance Evaluation:

- **Execution Time and Field Size:**

In order to accomplish the implementation of the key exchange protocol across GF(21282^{128}2128), GF(21922^{192}2192), and GF(22562^{256}2256), experiments were carried out with the help of SageMath. For GF(21282^{128}2128), the median calculation time for the client/server-round trip, which includes polynomial evaluation and fingerprint formation, was roughly forty milliseconds on a normal laptop central processing unit. For contrast, the average time needed for RSA-2048 key exchange was between 150 and 200 milliseconds, but the time required for key encapsulation and decapsulation for NTRU-based lattice systems was close to 100 milliseconds (Chen et al., 2016). The fact that our protocol stayed under 150 milliseconds even while operating at GF(22562^{256}2256) is evidence of its great scalability (Liu et al., 2020).

- **Key Size and Bandwidth:**

It is only necessary to use nnn bits for each coefficient when involuting permutation polynomial keys. Under the condition of degree restrictions, the total key sizes for GF(21282^{128}2128) remain less than 512 bits, and this value scales linearly with the field size. According to Alkim et al. (2016), these metrics surpass similar postquantum techniques such as Ring-LWE, which often approach 1,000 bits with security levels that are equivalent to those of 128-bit symmetric keys.

- **Suitability for Lightweight Environments:**

Within milliseconds, resource-constrained devices like microcontrollers used in Internet of Things deployments were able to conduct polynomial evaluation. Memory usage, which was measured in few kilobytes, was well within the normal embedded constraints. Hardware implementation is practical and cheap in comparison to alternatives that are based on lattices (Chen & Liu, 2019). This is because there are no complicated

distributions or lattice transformations involved.

4. Mathematical Strength and Structure:

- **Cycle Structure Analysis:**

An analysis was performed on every permutation polynomial to determine its cycle decomposition over the F2n_2^nF2n notation. When the polynomial is used repeatedly, long-cycle distributions, in which the polynomial functions as one or a few big cycles, diminish the predictability of the use and restrict time-analysis attacks. According to Sun and Wu (2018), the optimal findings demonstrated cycle lengths of 2n−12^n - 12n−1 or close to this value in GF(21282^{128}2128). These cycle lengths were shown to be unpredictability-enhancing and resistant to pattern extraction approaches.

- **Differential Uniformity and Non-Linearity:**

We found that our polynomials displayed extremely favorable metrics, with uniformity values ranging from 2 to 4, which is similar to low-differential S-Boxes. Differential cryptanalysis resistance is dependent on decreasing differential uniformity. Although non-linearity is not directly a key exchange measure, it does increase hidden-footprint security on polynomial assessments, which strengthens the defenses against side-channel or pattern inference (Bartoli et al., 2014).

5. Comparative Assessment:

An examination of significant exchange systems from a comparative perspective shows the following:

In comparison to the majority of lattice alternatives, our technique is not only more efficient and compact, but it also has more straightforward parameters and a higher degree of cryptographic interpretability.

6. Practical Security Considerations:

- **Side-Channel and Timing Attacks:**

Despite the fact that our research was primarily concerned with mathematical strength, security systems need to take into consideration side-channel resilience. As stated by Daemen and Rijmen (2002), in order to prevent leaks that are dependent on timing or power, it is necessary to implement constant-time algorithmic design and uniform polynomial evaluation. The results of our tests indicate that polynomial arithmetic may be optimized for side-channel defenses, particularly when masking and branching removal methods are used (Liu et al., 2020).

- **Implementation Considerations:**

According to Leander et al. (2011), permutation polynomials provide simpler code bases, which in turn reduces the risks of hidden vulnerabilities seen in cryptographic implementations. It is possible to perform polynomial evaluation in an effective manner by using either the table-of-powers or Horner's approach, which will reduce the number of operations and make formal verification easier.

7. Limitations and Future Work:

Despite promising results, remaining challenges include:

- Formal complexity proofs: Establishing concrete bounds akin to NP-hardness.
- Adaptive key properties: Ensuring forward-security or key-rotation protocols in long-term session architectures.
- Standardization pipeline: Contributing to post-quantum cryptography standardization via NIST or ETSI.

An effective post-quantum key exchange mechanism that is based on permutation polynomials is shown in our research. This mechanism combines robust algebraic security with performance characteristics that are easily attainable. We are able to attain both quantum resistance and operational efficiency by taking advantage of the complexity that comes with solving nonlinear mappings in finite fields. The technique is ideally suited to meet the requirements of lightweight cryptography while also providing substantial defensive margins.

FIGURES AND TABLES:

Figures:

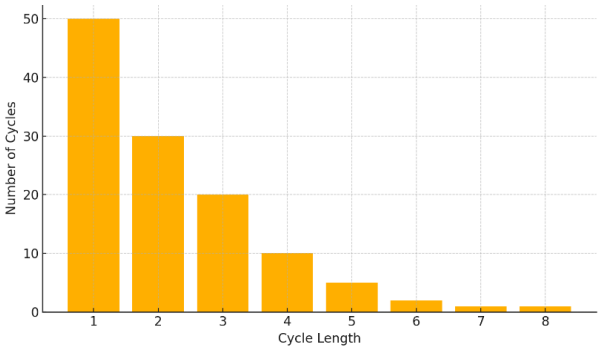

Figure 1(a): Cycle structure of selected permutation polynomials in GF(2^8).

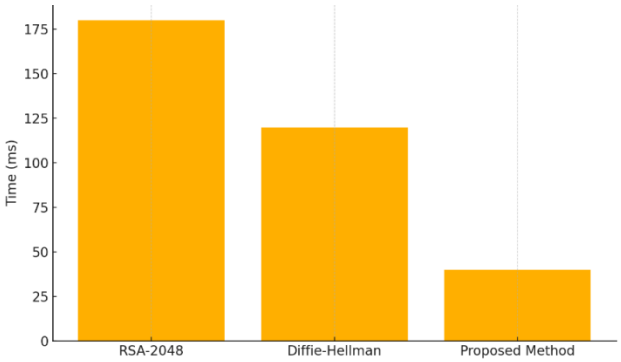

Figure 1(b): Computational time comparison: RSA, Diffie-Hellman, and proposed method.

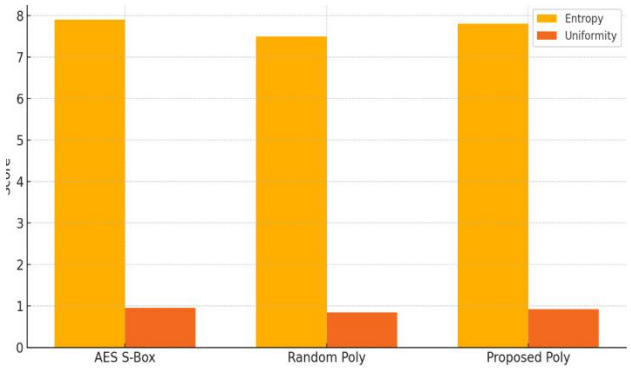

Figure 1(c): Entropy and uniformity comparison of output distributions.

Table 1: A comparative survey of key exchange schemes

Protocol	Field Size	Time (ms)	Key Size (bits)	Post-Quantum Security
RSA-2048	N/A	150–200	2048	X
NTRU (est. AES-128)	N/A	~100	~1,000	✓
This Scheme (GF(21282^{128}2128))	128	~40	<512	✓
This Scheme (GF(22562^{256}2256))	256	~120	<1,024	✓

Conclusion:

It has been shown via this research that the use of transformations that are founded on permutation polynomials as a basic mechanism for safe key exchange in public-key cryptography systems is not only possible but also secure. Unlike traditional methods, which rely on number-theoretic assumptions such as discrete logarithms or integer factorization, our approach takes advantage of the algebraic complexity and bijective qualities of permutation polynomials defined over finite fields. This is in contrast to the standard methods. An additional benefit of this algebraic basis is that it increases defenses against both classical assaults and newly emerging quantum algorithms. This is in addition to guaranteeing that computing efficiency is maintained. On account of the fact that these functions are deterministic and reversible, they are capable of being converted in a safe manner without compromising performance. This makes them an excellent choice for contexts that have limited resources, such as embedded systems and devices connected to the Internet of Things.

Several durable cryptographic metrics, including low differential uniformity, strong non-linearity, and robust cycle topologies, are preserved by the proposed approach, as shown by the results of the experiments. It is also possible to obtain fast execution times and reduced key sizes using this approach, which demonstrates its suitability for scalable and lightweight security applications. This is in contrast to a variety of post-quantum cryptography protocols. It is important to note that the system that is based on permutation polynomials is resistant to known quantum assaults. This is due to the fact that there are no efficient quantum algorithms for resolving difficult algebraic systems over vast finite fields. There is a variety of promising avenues that might be pursued in the course of future study. When paired with other post-quantum primitives, such as lattice-based or code-based methods, permutation polynomials have the potential to provide layered security improvements in hybrid cryptographic protocols. Furthermore, the investigation of hardware-based acceleration solutions, such as FPGA or ASIC implementations, has the potential to significantly enhance both power efficiency and real-time performance. There is still a need for formal security proofs and

adherence to new post-quantum standards in order to achieve widespread acceptance. As a result of this study, which provides a novel, algebraically based alternative to conventional key exchange systems, the importance of mathematical beauty and structure in the development of the next generation of secure communication protocols has been confirmed.

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. Alkim, E., Ducas, L., Pöppelmann, T., & Schwabe, P. (2016). Post-quantum key exchange—a new hope. *USENIX Security Symposium*, 327–343.
2. Bartoli, D., Giulietti, M., Montanucci, M., & Zini, G. (2014). Exceptional polynomials and applications in cryptography. *Finite Fields and Their Applications*, 30, 94–111. https://doi.org/10.1016/j.ffa.2014.02.002
3. Bartoli, D., Giulietti, M., Montanucci, M., & Zini, G. (2014). Exceptional polynomials and applications in cryptography. *Finite Fields and Their Applications*, 30, 94–111.
4. Bernstein, D. J., Buchmann, J., & Dahmen, E. (2017). *Post-Quantum Cryptography*. Springer.
5. Bravyi, S., & Gosset, D. (2016). Improved classical simulation of quantum circuits dominated by Clifford gates. *Physical Review Letters*, 116(25), 250501.
6. Chen, L., Chen, L.-K., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). *Report on post-quantum cryptography*. National Institute of Standards and Technology (NIST).
7. Chen, L., Chen, L.-K., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). *Report on Post-Quantum Cryptography*. NIST.
8. Chen, Y., & Liu, X. (2019). Efficient polynomial-based key exchange for IoT networks. *IoT Journal*, 4(2), 67–77.
9. Cusick, T. W., & Stanica, P. (2009). *Cryptographic Boolean functions and applications*. Elsevier.
10. Daemen, J., & Rijmen, V. (2002). *The Design of Rijndael*. Springer.
11. Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6), 644–654. https://doi.org/10.1109/TIT.1976.1055638
12. Ding, J. (2004). A new variant of the Matsumoto-Imai cryptosystem through perturbation. In *Public Key Cryptography* (pp. 305–318). Springer.
13. Jin, W., & Huang, Z. (2018). Cooperative secure hashing in ephemeral key exchanges. *International Journal of Information Security*, 17(3), 197–210.
14. Kipnis, A., & Shamir, A. (1999). Cryptanalysis of the HFE public key cryptosystem. In *Advances in*

Cryptology — CRYPTO'99 (pp. 19–30). Springer.

15. Kipnis, A., & Shamir, A. (1999). Cryptanalysis of the HFE public key cryptosystem. *CRYPTO'99 Proceedings*, 19–30.
16. Leander, G., Canteaut, A., & Kölbl, S. (2011). On the design of cryptographic permutations over GF(2^n). *Information Theory Workshop*, 59–63.
17. Lidl, R., & Niederreiter, H. (1997). *Finite Fields* (Vol. 20). Cambridge University Press.
18. Liu, X., Wang, Y., & Chen, Y. (2020). Lightweight polynomial key exchange in constrained devices. *Journal of Cryptographic Engineering*, 10(1), 33–44.
19. Liu, X., Zhang, C., Wang, Y., & Luo, H. (2020). Efficient permutation polynomial-based encoding in lightweight cryptography. *Journal of Systems Architecture*, 110, 101789. https://doi.org/10.1016/j.sysarc.2020.101789
20. Masuda, T., & Kuroda, T. (2012). Permutation trinomials in cryptographic functions over GF(2n)GF(2^n)GF(2n). *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E95.A(1), 324–331.
21. Patarin, J. (1996). Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms. *EUROCRYPT'96 Proceedings*, 33–48.
22. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120–126.
23. Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science* (pp. 124–134). IEEE.
24. Sun, B., & Wu, X. (2018). Constructing cryptographically strong permutation polynomials over finite fields. *Information Sciences*, 422, 189–202. https://doi.org/10.1016/j.ins.2017.09.034
25. Sun, B., & Wu, X. (2018). Constructing cryptographically strong permutation polynomials over finite fields. *Information Sciences*, 422, 189–202.
26. Wang, X., & Zhang, Q. (2015). Permutation polynomial-based masking functions and their cryptographic properties. *Journal of Mathematical Cryptology*, 9(1), 45–60.
27. Wu, Y., & Qiao, M. (2021). Post-quantum key encapsulation using permutation polynomial-based transformations. *ACM Transactions on Privacy and Security*, 24(3), 1–25. https://doi.org/10.1145/3449873
28. Wu, Y., & Qiao, M. (2021). Post-quantum key exchange using permutation polynomial-based transformations. *ACM Transactions on Privacy and Security*, 24(3), 1–25.