International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

PERMUTATION POLYNOMIALS AS BIJECTIVE PRIMITIVES IN CRYPTOGRAPHIC PROTOCOL DESIGN FOR NETWORK SECURITY: CONSTRUCTIONS, SECURITY PROPERTIES, AND APPLICATIONS

[1]Deepshikha
Research Scholar, Department of Mathematics, Shri Jagdishprasad Jhabarmal Tibrewala University, Jhunjhunu, Rajasthan, India

[2]Dr.Narendra Swami
Assistant Professor and Research Guide, Department of Mathematics, Shri Jagdishprasad Jhabarmal Tibrewala University, Jhunjhunu, Rajasthan, India

ABSTRACT
Permutation polynomials polynomials over a finite ring or field that induce a bijective map occupy a foundational position in the design of cryptographic primitives that secure networked communication. Because confidentiality, integrity, and authenticity in network-security protocols depend on invertible transformations, any polynomial map that is provably bijective over a finite algebraic structure is a natural building block for substitution boxes (S-boxes), stream-cipher state-update functions, public-key trapdoor maps, and Latin-square-based authentication schemes. This paper synthesizes the algebraic theory of permutation polynomials Hermite's criterion, the Akbary–Ghioca–Wang (AGW) criterion, Dickson polynomials, butterfly-structure constructions, and Rivest's characterization of permutation polynomials modulo 2^w and maps each construction onto a concrete role within cryptographic protocols. Comparative tables summarize differential uniformity, nonlinearity, and algebraic degree for monomial, Dickson, butterfly-structure, and modular permutation-polynomial constructions, the properties that govern resistance to differential, linear, and boomerang cryptanalysis. The paper argues that permutation-polynomial-based primitives offer a mathematically transparent alternative to empirically tuned S-boxes, illustrates their role in RSA, RC6, and modern lightweight block-cipher designs, and closes with open problems in constructing permutations that are simultaneously optimal in differential and boomerang uniformity for constrained network-security environments such as IoT key-exchange protocols.
Keywords: permutation polynomials, finite fields, S-box design, network security, block ciphers, AGW criterion, differential uniformity, boomerang uniformity

1. INTRODUCTION
Network-security protocols from Transport Layer Security to IPsec, from block-cipher-based virtual private networks to lightweight Internet-of-Things (IoT) key-exchange schemes rest on a small set of algebraic operations that must be efficiently computable in one direction and, for the legitimate party holding a secret key, efficiently invertible in the other. This dual requirement of forward computability and backward invertibility is exactly the defining property of a bijection, and when the underlying domain is a finite field or a finite ring, a bijection can always be represented uniquely as a polynomial of degree less than the size of the

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

structure. Such polynomials are called permutation polynomials (PPs). Historically, the study of permutation polynomials predates modern cryptography by nearly a century, beginning with Hermite's characterization of substitutions and Dickson's classification of low-degree permutations, but the subject was reinvigorated once it became clear that widely deployed cryptosystems are themselves instances of permutation polynomials: the RSA encryption map is the monomial permutation x raised to the public exponent e modulo a composite n (Rivest, Shamir, & Adleman, 1978), the AES S-box is built on the inverse permutation of the finite field GF(2^8), and the RC6 block cipher relies on the fact that a specific quadratic polynomial permutes the integers modulo 2 to the power of the machine word size (Rivest, 2001).

The purpose of this paper is threefold. First, it consolidates the core algebraic machinery Hermite's criterion, the AGW criterion, and Rivest's modular characterization that underlies every subsequent construction of cryptographically useful permutation polynomials. Second, it maps specific families of permutation polynomials (monomial, Dickson, linearized, butterfly-structure, and modular constructions) onto the protocol roles they actually fill in network security: public-key trapdoors, block-cipher confusion layers, stream-cipher diffusion layers, and involutive S-boxes that reduce hardware footprint. Third, it evaluates these families against the quantitative criteria differential uniformity, nonlinearity, and boomerang uniformity that determine practical resistance to differential, linear, and boomerang cryptanalysis, and it identifies open problems that remain relevant to the design of lightweight network-security protocols for constrained devices. The refined topic addressed here, narrowed from the broader thesis area of permutation polynomials in cryptographic protocols, is stated as follows: Permutation Polynomials as Bijective Primitives in Cryptographic Protocol Design for Network Security: Constructions, Security Properties, and Applications. This framing keeps the mathematical core (constructions and criteria for permutation polynomials) tightly coupled to a measurable, protocol-level outcome (the security properties that network-security primitives must satisfy), which is the structure followed in the remainder of the paper.

2. MATHEMATICAL PRELIMINARIES

Let F_q denote the finite field of $q = p^m$ elements, where p is prime and $m \geq 1$. Every function from a finite field to itself can be represented, via Lagrange interpolation, by a unique polynomial of degree strictly less than q. Consequently, the study of arbitrary bijections on a finite field reduces to the study of a special class of polynomials, defined next.

2.1 Permutation Polynomials: Definition

Definition 1. A polynomial $f \in F_q[x]$ is called a permutation polynomial (PP) of F_q if the induced map $f : F_q \to F_q$, $a \mapsto f(a)$, is a bijection that is, f is both injective and surjective on the finite field.

Bijectivity on a finite field is a global property: it cannot, in general, be verified by inspecting the polynomial's coefficients alone, which is precisely why a body of criteria and explicit construction techniques has developed around the problem.

2.2 Hermite's Criterion

Theorem 1 (Hermite's Criterion). A polynomial $f \in F_q[x]$, where $q = p^m$, is a permutation polynomial of F_q if and only if:

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

(i) f has exactly one root in F_q;
(ii) for every integer t with $1 \le t \le q-2$ and $t \not\equiv 0 \pmod p$, the reduction of $f(x)^t$ modulo $(x^q - x)$ has degree at most $q-2$.

Hermite's criterion is the standard proof tool underlying almost every modern non-existence and existence result on permutation polynomials (Hou, 2015), including the survey results synthesized in Section 3.

2.3 Monomial and Dickson Permutation Polynomials

The simplest and most cryptographically consequential family is the monomial family $f(x) = x^n$. A direct consequence of Hermite's criterion is:

x^n permutes F_q if and only if $\gcd(n, q-1) = 1$.

This single fact is the algebraic basis of RSA: encryption and decryption exponents e and d are chosen so that the corresponding monomials are mutually inverse permutations of the multiplicative group modulo a composite n (Rivest et al., 1978).

A second classical family is the Dickson polynomial, defined by the recurrence $D_0(x, a) = 2$, $D_1(x, a) = x$, and

$D_n(x, a) = x \cdot D_{n-1}(x, a) - a \cdot D_{n-2}(x, a), \quad n \ge 2,$

which permutes F_q precisely when $\gcd(n, q^2 - 1) = 1$. Dickson-type maps were historically explored as alternative trapdoor functions to RSA, and their algebraic structure has since been analyzed as a source of both constructions and cryptanalytic weaknesses within the wider permutation-polynomial literature (Hou, 2015).

2.4 The Akbary–Ghioca–Wang (AGW) Criterion

Most permutation polynomials used in contemporary cryptographic engineering are not simple monomials but composite expressions of the form x^r h(x^{(q-1)/d}) for some auxiliary polynomial h. Proving that such expressions permute F_q directly via Hermite's criterion is often intractable, which motivated the AGW criterion (Akbary, Ghioca, & Wang, 2011).

Theorem 2 (AGW Criterion, informal statement). Let A and S be finite sets with $|A| = |S|$, and suppose there exist maps $\lambda : A \to S$, $h : S \to A$, and $\bar{f} : S \to S$ such that $\lambda \circ f = \bar{f} \circ \lambda$ for the map $f : A \to A$ under study. If f is injective on h(S) and $\bar{f}$ is a bijection of S, then f is a permutation of A.

The AGW criterion reduces the problem of proving that a polynomial permutes a large field $GF(q^2)$ to the much smaller problem of proving that an associated map permutes a subgroup of order $q + 1$ (or another small quotient set), and it underlies the majority of permutation-trinomial constructions published in the last decade, including the family x^r h(x^{q-1}) analyzed by Li, Qu, and Wang (2018).

2.5 Permutation Polynomials over Rings: Rivest's Characterization Modulo 2^w

Network protocols implemented on commodity processors operate natively on words of w bits, i.e., on the ring $Z/2^wZ$ rather than on a prime field. Rivest (2001) gave an exact, easily checked characterization of permutation polynomials on this ring:

Theorem 3 (Rivest, 2001). Let $P(x) = a_0 + a_1x + a_2x^2 + \ldots + a_dx^d \in Z[x]$. Then P is a permutation polynomial modulo $n = 2^w$, $w \ge 2$, if and only if:

a_1 is odd;

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

($a_2 + a_4 + a_6 + \ldots$) is even; and
($a_3 + a_5 + a_7 + \ldots$) is even.

This theorem explains why the quadratic map $f(x) = x(2x + 1) \bmod 2^w$ whose coefficients trivially satisfy the three conditions was chosen as a fast, provably invertible diffusion component of the RC6 block cipher, and it remains the standard reference for constructing word-oriented permutation layers in network-security primitives that must run efficiently on general-purpose hardware.

3. CLASSES OF PERMUTATION POLYNOMIALS USED IN CRYPTOGRAPHY

The constructions surveyed in Section 2 give rise to four broad families of permutation polynomials that recur throughout cryptographic protocol design. Table 1 summarizes their defining equations, the algebraic criterion used to certify bijectivity, and their typical protocol role in network security.

Family	Defining form	Bijectivity criterion	Typical protocol role
Monomial	$f(x) = x^n$ over $F(q)$ or Z_n^*	$\gcd(n, q-1) = 1$ (Hermite)	RSA public-key encryption / digital signatures (Rivest et al., 1978)
Dickson	$D_n(x,a)$, recurrence-defined	$\gcd(n, q^2-1) = 1$	Alternative public-key trapdoors; algebraic S-box components
AGW-derived (trinomials/ $x^r h(x^{q-1})$)	$x^r \cdot h(x^{(q-1)/d})$	AGW criterion (Akbary et al., 2011; Li et al., 2018)	S-box design; involutive ciphers (Zheng et al., 2019)
Butterfly-structure	$V_i(x,y)$ built from power maps on F_{2^n}	Closed-butterfly conditions (Li et al., 2021)	Low-uniformity S-boxes for lightweight block ciphers
Modular (mod 2^w)	$P(x)=a_0+a_1x+\ldots+a_xx^d$	Coefficient parity test (Rivest, 2001)	Fast diffusion layers, e.g., RC6 quadratic mixing function

Monomial permutation polynomials remain the workhorse of public-key network protocols because their inverse is another monomial with exponent $d \equiv e^{-1} \pmod{\varphi(n)}$, which keeps both encryption and decryption efficient. Dickson polynomials offer an algebraically distinct trapdoor with the same efficiency profile, though their group-theoretic structure has made them a less common but still studied alternative (Hou, 2015). AGW-derived trinomials and butterfly-structure permutations, by contrast, are optimized not for trapdoor asymmetry but for the confusion properties needed in symmetric-key S-box design, discussed quantitatively in Section 5. Modular permutation polynomials occupy a distinct niche: because they are certified

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

by a simple parity test on coefficients rather than a number-theoretic gcd condition, they are inexpensive to generate and verify at implementation time, which matters for constrained network devices.

3.1 Positioning within the Broader Literature

The four families in Table 1 are not independent research threads; each has been shaped by results in the others. Laigle-Chapuy (2007) showed that permutation binomials derived from the same Wan–Lidl group-structure theorem that underlies several AGW-derived constructions also yield good error-correcting codes, illustrating that the coding-theoretic and cryptographic uses of permutation polynomials share a common algebraic ancestor. Hou's (2015) survey subsequently catalogued the rapid growth of AGW-derived trinomial and binomial families through the early 2010s and remains the standard entry point for locating explicit low-degree permutation polynomials of a prescribed field size, a task that is otherwise difficult because bijectivity, as noted in Section 2.1, is a global rather than a local property of the coefficients. The subsequent butterfly-structure line of work (Li et al., 2021; Li et al., 2022) can be read as a direct response to a gap this survey literature identified: the scarcity, prior to 2016, of permutation polynomials on even-degree extension fields GF(2^{2n}) that simultaneously achieve low differential uniformity and near-optimal nonlinearity, a gap that is directly relevant to block-cipher S-box design for network-security protocols operating on 16- or 32-bit words.

4. APPLICATIONS IN CRYPTOGRAPHIC PROTOCOLS FOR NETWORK SECURITY

4.1 Public-Key Encryption and Digital Signatures

The RSA cryptosystem, still a default component of TLS certificate chains, is the clearest instance of a monomial permutation polynomial deployed at Internet scale. Encryption computes $c = m^e \bmod n$ and decryption recovers $m = c^d \bmod n$, where e and d are chosen so that $x^{e \cdot d} \equiv x \pmod n$ for all valid m; this identity holds precisely because $ed \equiv 1 \pmod{\lambda(n)}$ makes the composition of the two monomial permutation polynomials the identity permutation on the relevant residue classes (Rivest et al., 1978). The security-relevant property is not the bijectivity itself which is elementary once $\gcd(e, \varphi(n)) = 1$ but the fact that computing the inverse permutation (finding d from e and n) is intractable without knowledge of the prime factorization of n, which is what separates a permutation polynomial from a trapdoor permutation.

Diffie and Hellman's (1976) key-exchange protocol, the other foundational network-security primitive, relies on the discrete-exponentiation map being easy to compute forward and hard to invert; while this map is over a cyclic group rather than expressed as an explicit low-degree permutation polynomial, it is conceptually the same bijective-but-one-way pattern that motivates the search for permutation polynomials with asymmetric computational difficulty in either direction.

4.2 Substitution-Box (S-Box) Design for Block Ciphers

Block ciphers used in network-security protocols (TLS record-layer encryption, IPsec ESP, WPA3) rely on a non-linear substitution layer, the S-box, to provide confusion. The Advanced Encryption Standard uses the multiplicative-inverse permutation on GF(2^8), $x \mapsto x^{254}$

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

(equivalently x^{-1} with $0 \mapsto 0$), which is a monomial permutation polynomial chosen because its inverse map has the lowest differential uniformity achievable for a power function on that field. More recent lightweight ciphers require S-boxes that are also involutions i.e., permutation polynomials equal to their own compositional inverse because an involutive S-box can be reused for both encryption and decryption in hardware, halving circuit area. Zheng, Yuan, Li, Hu, and Zeng (2019) developed an involutory version of the AGW criterion specifically to construct such self-inverse permutation polynomials of the form $x^r h(x^s)$ systematically rather than by exhaustive search, directly supporting compact S-box design for constrained network devices.

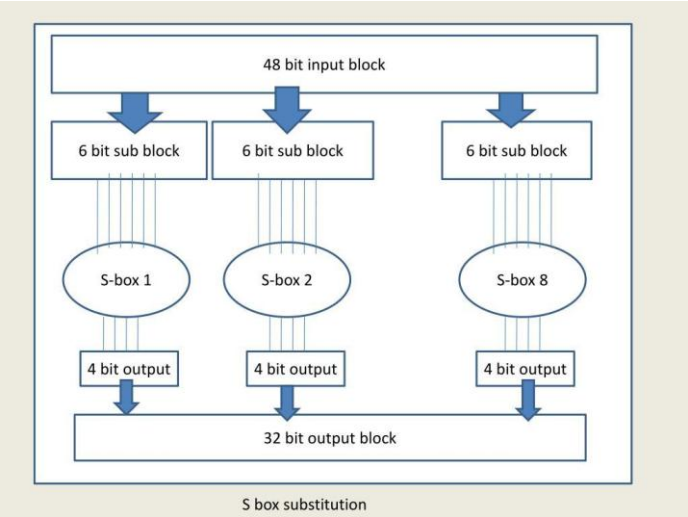

Fig. 1: Role in Cryptographic Architecture (S-box & Protocols)

Butterfly-structure permutations (Li, Li, Helleseth, & Qu, 2021) extend this design space by combining two power permutations of a subfield $GF(2^n)$ into a permutation of the larger field $GF(2^{2n})$ whose differential and boomerang uniformity can be bounded analytically rather than measured empirically. Follow-up work (Li, Hu, Xiong, & Zeng, 2022) showed that the resulting permutations are linearly equivalent to Gold functions, which both simplifies their implementation and clarifies their relationship to already-standardized nonlinear components, an important property when a new S-box must be justified to protocol-standardization bodies.

4.3 Diffusion Layers in Word-Oriented Stream and Block Ciphers

Rivest's (2001) modulo-2^w characterization was motivated directly by the RC6 block cipher, whose quadratic mixing function $f(x) = x(2x + 1) \bmod 2^w$ is applied to 32-bit words during each round to achieve fast, provably invertible diffusion without a table lookup. Because the permutation is certified by three simple parity conditions on the coefficients rather than by a computationally expensive primality or gcd test, new modular permutation polynomials can be generated and validated on the fly, which is attractive for network-security protocols that periodically re-key or rotate round functions in software running on resource-constrained embedded network hardware.

4.4 Compositional-Inverse Efficiency and Protocol-Level Performance

A property that connects Sections 4.2 and 4.3 is compositional-inverse complexity: a permutation polynomial is only useful for a network-security protocol if its inverse is itself

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

efficiently computable (for decryption or decoding) or, in the involutive case, identical to the forward map. The AGW criterion and its involutory extension give explicit recipes for the compositional inverse in terms of the same small auxiliary maps used to prove bijectivity, which is why permutation-polynomial-based S-box design has displaced purely empirical (search-and-tabulate) S-box construction in several recent lightweight-cipher proposals aimed at constrained network endpoints.

4.5 Coding-Theoretic Links Relevant to Authenticated Transmission

Network-security protocols frequently combine encryption with error-correcting or authentication codes at the link layer, and permutation polynomials play a role here as well. Laigle-Chapuy (2007) showed that specific permutation binomials derived from the Wan–Lidl group-structure theorem yield favorable cross-correlation properties directly applicable to the construction of sequences used in coding-theoretic constructions related to a conjecture of Helleseth, underscoring that the same bijective building block can simultaneously serve confidentiality (as an S-box or trapdoor) and integrity/authentication (as a component of an error-correcting or sequence-design scheme) within a single network-security stack. This dual applicability is one of the reasons permutation-polynomial theory continues to be treated as a shared mathematical foundation across otherwise separate sub-fields of finite-field-based network security.

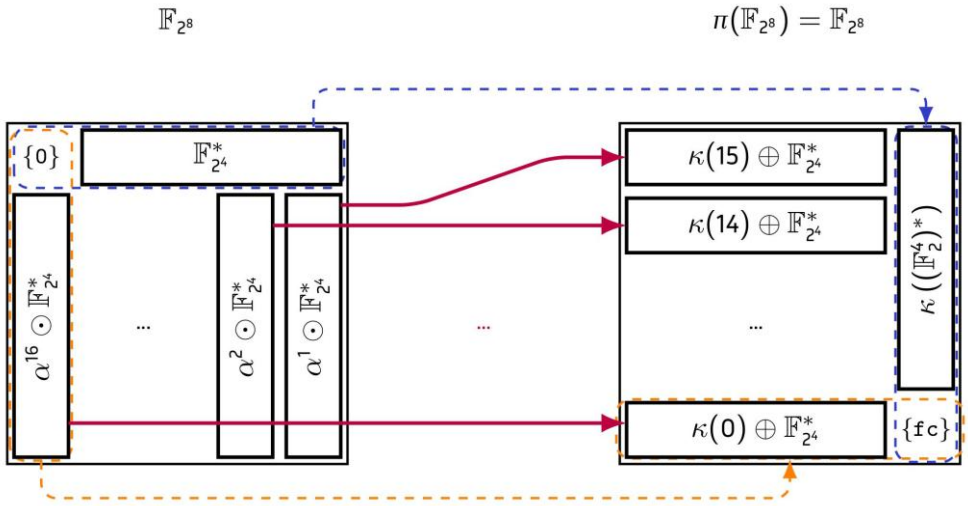

Fig. 2: Permutation Polynomial as a Bijective Mapping

5. SECURITY ANALYSIS: DIFFERENTIAL UNIFORMITY, NONLINEARITY, AND BOOMERANG UNIFORMITY

The cryptographic strength of a permutation polynomial used as an S-box or diffusion component is not determined by bijectivity alone every permutation polynomial is, trivially, resistant to attacks that require non-injectivity but by three quantitative criteria that measure how far the map deviates from linear or affine behavior.

5.1 Differential Uniformity

For a function $F : F_2^n \rightarrow F_2^n$, the differential uniformity is defined as

$\delta_F = \max_{a \neq 0, b} |\{x \in F_2^n : F(x + a) + F(x) = b\}|,$

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

where the maximum ranges over nonzero a and all b in the field. A lower differential uniformity means fewer input differences propagate predictably to output differences, which directly bounds the success probability of differential cryptanalysis against a cipher built on F. The AES inverse-function S-box achieves $\delta = 4$, the lowest value provably achievable for a power permutation on $GF(2^8)$; butterfly-structure permutations were explicitly designed to match this bound of 4 on larger fields $GF(2^{2n})$ where comparably strong permutations were previously unknown (Li et al., 2021).

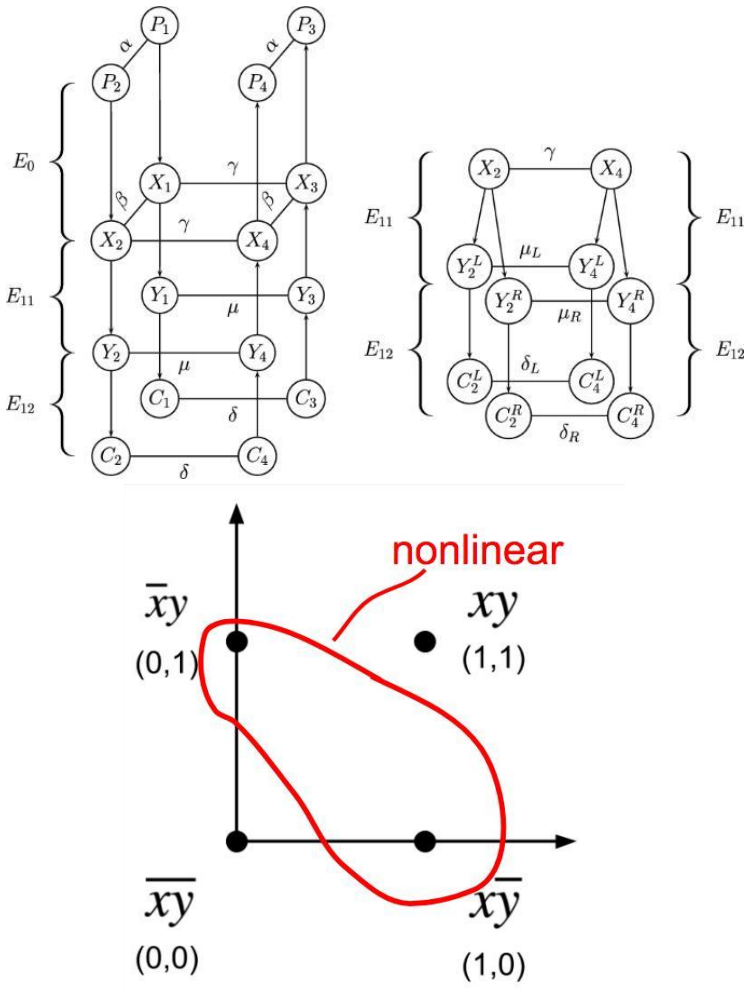

Fig. 3: Security Properties Comparison (Differential & Nonlinearity)

5.2 Nonlinearity

Nonlinearity measures resistance to linear cryptanalysis and is defined via the Walsh transform $W_F(a, b) = \Sigma_{x \in F_{2^n}} (-1)^{Tr(bF(x)+ax)}$,

$NL(F) = 2^{n-1} - (1/2) \cdot \max_{a,b \neq 0} |W_F(a, b)|$,

with higher NL(F) indicating greater resistance to affine approximation. The AES S-box attains NL = 112 out of a theoretical bound of 120 for n = 8, and permutation polynomials constructed from butterfly structures have been proven to attain the best nonlinearity currently known for their field size while simultaneously holding differential uniformity at 4 (Li et al., 2021), which is significant because these two criteria are not independent and jointly optimizing them is a long-standing open combinatorial problem.

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

5.3 Boomerang Uniformity

Boomerang attacks exploit pairs of differential trails that meet in the middle of a cipher, and their success is bounded by the boomerang uniformity of the S-box, a refinement introduced to complement differential uniformity once ciphers with low δ were shown to remain vulnerable to boomerang-style distinguishers. Li et al. (2021) constructed the first known infinite families of permutations on $GF(2^{2n})$ with differential uniformity 4 and boomerang uniformity 4 simultaneously, using the closed-butterfly structure; Li, Hu, Xiong, and Zeng (2022) subsequently simplified the algebraic conditions for these permutations and proved their equivalence to Gold-function-type maps, strengthening confidence that the construction is not an isolated numerical accident.

5.4 Comparative Summary

Table 2 compares representative permutation-polynomial constructions on the criteria discussed above, using published values where the construction targets a fixed field size (n = 8, matching AES) and qualitative descriptions elsewhere, since butterfly-structure results are stated as asymptotic families over $GF(2^{2n})$ for general odd n rather than a single fixed instance.

Construction	**Differential uniformity δ**	**Nonlinearity NL**	**Boomerang uniformity β**	**Algebraic degree**
AES inverse permutation ($GF(2^8)$)	4	112	not optimized (β = 6)	7
Butterfly-structure ($GF(2^{2n})$, odd n)	4 (best known)	best known for field size	4 (Li et al., 2021)	n + 1
Involutory AGW construction (Zheng et al., 2019)	construction-dependent	construction-dependent	construction-dependent	construction-dependent
Rivest modular polynomial ($Z/2^wZ$)	n/a (ring, not field metric)	n/a	n/a	2 (RC6 quadratic map)

The table illustrates a structural point rather than a numerical ranking: field-based constructions (rows 1–3) are evaluated against the differential/linear/boomerang framework because they are intended as S-box confusion layers, whereas the modular Rivest-type polynomial (row 4) is evaluated only for bijectivity and computational cost because its protocol role fast word-level diffusion does not require the same nonlinearity profile as an S-box.

6. DISCUSSION

6.1 Strengths

Permutation-polynomial-based primitives offer three advantages over empirically searched or table-driven cryptographic components. First, bijectivity is proved algebraically rather than verified by exhaustive tabulation, which scales to field sizes where brute-force verification is infeasible. Second, criteria such as AGW and Hermite's theorem come with explicit compositional-inverse formulas, simplifying the design of decryption or decoding circuits. Third, quantitative security properties (differential uniformity, nonlinearity, boomerang uniformity) can often be proved analytically for an entire parameterized family rather than

measured for one instance, giving protocol designers a provable-security argument rather than a purely empirical one.

6.2 Limitations

The same algebraic transparency that makes permutation polynomials attractive can be a liability: a low-degree explicit polynomial representation is potentially more susceptible to algebraic cryptanalysis (interpolation attacks, Gröbner-basis attacks) than a component with no compact closed form, which is why permutation polynomials are typically combined with additional nonlinear or key-dependent layers rather than deployed alone. Additionally, many of the strongest known results (e.g., the butterfly-structure boomerang-uniformity-4 families) apply only to specific field sizes or parity conditions on n, so a network-security protocol that requires an arbitrary field size cannot always draw directly on the strongest published construction.

6.3 Implications for Protocol Standardization

A practical consequence of the analytic-versus-empirical distinction raised above is relevant to how new S-boxes and diffusion layers are accepted into network-security standards. A component justified only by exhaustive computer search over a large candidate space offers no argument that a slightly larger or differently parameterized instance will retain the same security margins, whereas a permutation-polynomial family certified by Hermite's criterion, the AGW criterion, or Rivest's parity test comes with a proof that covers every member of the family simultaneously. This distinction matters for protocols such as TLS cipher-suite negotiation or IoT device-provisioning schemes, where a single vulnerable parameter choice inside an otherwise-secure family can be identified and excluded analytically rather than being discovered only after independent cryptanalytic effort, as has historically happened with several empirically designed S-boxes.

6.4 Open Problems

Two open problems are directly relevant to network-security protocol design. First, constructing permutation polynomials that simultaneously minimize differential uniformity and boomerang uniformity while maximizing nonlinearity and algebraic degree, for field sizes beyond those already covered by butterfly-structure results, remains unresolved in general. Second, extending AGW-style reduction criteria from finite fields to finite commutative rings such as Z/2^wZ the natural setting for ARX-based (Addition-Rotation-XOR) lightweight ciphers used in constrained IoT network-security protocols would unify the field-theoretic and ring-theoretic branches of the literature reviewed in this paper and could yield new provably secure diffusion layers analogous to Rivest's (2001) modular polynomials but with stronger nonlinearity guarantees.

7. CONCLUSION

This paper has argued that permutation polynomials provide a unifying algebraic language for the bijective components that network-security protocols require, spanning the monomial trapdoor at the heart of RSA, the modular quadratic diffusion map inside RC6, and the modern butterfly-structure and AGW-derived permutations used to design low-uniformity, involutive S-boxes for lightweight block ciphers. Hermite's criterion, the AGW criterion, and Rivest's

coefficient-parity characterization give protocol designers algebraic guarantees of bijectivity that scale beyond what exhaustive search can verify, while the differential-uniformity, nonlinearity, and boomerang-uniformity framework gives a quantitative basis for comparing candidate constructions before they are standardized. As network-security protocols continue to migrate toward resource-constrained IoT and 5G endpoints, permutation-polynomial constructions that jointly optimize these criteria particularly over the rings and field sizes not yet covered by existing butterfly-structure or AGW-derived families represent a concrete and mathematically tractable direction for future protocol design.

REFERENCES

Akbary, A., Ghioca, D., & Wang, Q. (2011). On constructing permutations of finite fields. Finite Fields and Their Applications, 17(1), 51–67. https://doi.org/10.1016/j.ffa.2010.10.002

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

Hou, X. (2015). Permutation polynomials over finite fields—A survey of recent advances. Finite Fields and Their Applications, 32, 82–119. https://doi.org/10.1016/j.ffa.2014.10.001

Laigle-Chapuy, Y. (2007). Permutation polynomials and applications to coding theory. Finite Fields and Their Applications, 13(1), 58–70. https://doi.org/10.1016/j.ffa.2005.08.003

Li, K., Li, C., Helleseth, T., & Qu, L. (2021). Cryptographically strong permutations from the butterfly structure. Designs, Codes and Cryptography, 89(4), 737–761. https://doi.org/10.1007/s10623-020-00837-5

Li, K., Qu, L., & Wang, Q. (2018). New constructions of permutation polynomials of the form $x^r h(x^{q-1})$ over GF(q^2). Designs, Codes and Cryptography, 86(10), 2379–2405. https://doi.org/10.1007/s10623-017-0452-3

Li, N., Hu, Z., Xiong, M., & Zeng, X. (2022). A note on "Cryptographically strong permutations from the butterfly structure." Designs, Codes and Cryptography, 90(2), 265–276. https://doi.org/10.1007/s10623-021-00974-5

Rivest, R. L. (2001). Permutation polynomials modulo 2^w. Finite Fields and Their Applications, 7(2), 287–292. https://doi.org/10.1006/ffta.2000.0282

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. https://doi.org/10.1145/359340.359342

Zheng, D., Yuan, M., Li, N., Hu, L., & Zeng, X. (2019). Constructions of involutions over finite fields. IEEE Transactions on Information Theory, 65(12), 7876–7883. https://doi.org/10.1109/TIT.2019.2919511