

Every keyed DNA operation is affine: algebraic limits of DNA diffusion layers in image encryption

Ihab Shakir

ehabaldefae6@gmail.com

University of Tabriz

Hossein Kheiri

University of Tabriz

Article

Keywords: Image encryption, DNA coding, Algebraic degree, Cryptanalysis, Diffusion layer, Boolean functions

Posted Date: October 26th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-10968467/v1>

License:   This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Additional Declarations: No competing interests reported.

Every keyed DNA operation is affine: algebraic limits of DNA diffusion layers in image encryption

Ihab Shakir^{1*} and Hossein Kheiri^{1*}

^{1*}Department of Applied Mathematics, Faculty of Mathematics, Statistics and Computer Science, University of Tabriz, Tabriz, Iran.

*Corresponding author(s). E-mail(s): ehabaldefae6@gmail.com;
h-kheiri@tabrizu.ac.ir;

Abstract

For over fifteen years, image encryption schemes have combined chaotic systems with deoxyribonucleic acid (DNA) coding, and their DNA diffusion layers have been broken, scheme after scheme, by strikingly similar attacks. This paper shows that the similarity is structural. Because the DNA alphabet has four letters, every bijection of it is affine over the binary field: every decryptable keyed DNA operation—all **331,776** admissible tables, under all **24** encoding rules, any schedule and any number of rounds—has algebraic degree one, and the published algebraic cryptanalyses of such layers are special cases of this single fact. With two plaintext-dependent operands the degree reaches two but no more; differential uniformity and nonlinearity remain at their worst possible values for every admissible operation; and four is the largest alphabet size for which the obstruction holds. We further diagnose a chained construction adopted in four recent schemes, half of whose operation menu is affine and whose associative addition accumulates $2^k - 1$ image-independent linear structures, and give a zero-cost replacement, verified on medical images, that removes both defects. The standard statistical battery is blind to every one of these distinctions. The algebraic degree, computable in seconds, is the number that would expose them, and we argue it belongs in the evaluation tables of this literature. All enumerations are exhaustive and machine-checked, and the verification package is archived.

Keywords: Image encryption, DNA coding, Algebraic degree, Cryptanalysis, Diffusion layer, Boolean functions

MSC Classification: 94A60 , 06E30 , 11T71 , 94A08 , 68P25

1 Introduction

Paper after paper on DNA-based image encryption states the same count. Of the $4! = 24$ ways to assign the four nucleotide bases to the four 2-bit values, eight satisfy the Watson–Crick complementarity constraint, and the scheme at hand selects among those eight [1–4]. For fifteen years this number has been read as an inventory of encoding options. Read instead as the order of a group, it says something else entirely: 24 is the order of the affine group $\text{AGL}(2, 2)$, and since it is also the number of *all* bijections of a four-letter alphabet, every bijection of the DNA alphabet is affine over $\mathbb{F}_2$. That coincidence—and it is not one—forecloses the nonlinearity of every keyed DNA operation ever proposed, and, we will argue, explains a decade of near-identical cryptanalyses.

DNA coding entered image encryption as a lightweight symbol layer combined with chaotic generators: pixels are encoded as base sequences, combined with chaotic key material through table-defined operations—DNA addition, subtraction, XOR, XNOR—and decoded, with the rule and operation indices themselves often driven by chaotic sequences [5–8]. The security argument offered for such schemes is, almost without exception, statistical: ciphertext entropy, histogram uniformity, adjacent-pixel correlation, and the plaintext-sensitivity scores NPCR and UACI [9].

The record of these layers under actual cryptanalysis is uniform. The DNA-addition scheme of [10] was broken in [11]; the scheme of [12] was reduced to an equivalent description and its key space collapsed in [13]; the codec structure of a spatiotemporal-chaos scheme was reduced to a bitwise complement and the scheme broken with nine chosen plaintexts in [4]; DNA encryption was shown to synthesize into ordinary S-box substitution in [14]. Solak had already isolated the pattern in 2011: statistical results, however good, “cannot hide the algebraic weaknesses inherent in the cipher”, and ciphers that are *inadvertently linear* fall to elementary linear algebra [15]. On the neighbouring cellular-automata layer the design-side lesson was even drawn explicitly: Ping et al. classified the elementary CA rules and built ciphers from the non-affine balanced ones [16, 17].

However, each of these analyses concerns one scheme, and the design-side criterion was never carried across to the DNA layer itself. None of the cryptanalyses asks whether the failure it exploits is an accident of the scheme under attack or a property of the design space; no design paper, in a corpus of 122 examined here, computes or even names the algebraic degree of its DNA layer; and the constructions keep appearing—including a chained variant, adopted independently in four recent papers [18–21], that comes within one choice of escaping the problem and then makes that choice at random. The question this paper answers is the structural one: *what algebraic degrees are attainable, by any construction whatsoever, inside the DNA design space—and what follows for the schemes being published now?*

The contributions are the following.

1. **An impossibility theorem** (Section 3): every keyed DNA operation satisfying the minimum requirement of decryptability is affine—uniformly over all 331,776 admissible operation tables, all 24 encoding and decoding rules, all schedules, and

all round counts. The proof is four lines; the published algebraic collapses of [4, 13, 14] are recovered as special cases.

2. **A ceiling theorem** (Section 4): with two plaintext-dependent operands—the only escape the alphabet permits—the degree reaches 2 on exactly 432 of the 576 admissible operations and can go no higher, while differential uniformity and nonlinearity are pinned at their worst possible values on all 576.
3. **A boundary theorem** (Section 5): $\text{AGL}(m, 2) = \text{Sym}$ precisely for $m \leq 2$, so the four-letter alphabet of DNA coding is the largest on which the impossibility operates; the obstruction belongs to the alphabet size, not to the operations.
4. **A diagnosis of the chained designs** (Section 6): in the four recent schemes, half of the operation menu is affine, leaving an expected half of the chaining steps without nonlinearity; and the $\mathbb{Z}_4$ addition they share is associative, which collapses the chain to a prefix sum and accumulates $2^k - 1$ image-independent linear structures.
5. **A zero-cost replacement** (Section 6.3): a non-associative degree-2 operation of identical table size and decryption cost under which the chain degree grows with its length and the linear structures hold constant at three; decryption is verified over 20,000 random chains.
6. **An experimental and bibliometric demonstration** (Section 7): the full statistical battery of this literature cannot distinguish any of the above variants, whereas an encoding-independent degree/DU/NL certificate—applied to the entire published operation set in under a second—separates them at once; the avalanche the four papers report is produced by hash re-seeding rather than by the DNA layer; and in a corpus of 154 documents the algebraic vocabulary carried by 70% of the field’s reference works does not reach its 122 design papers, in which *algebraic degree* and *differential uniformity* never occur at all and *nonlinearity* is applied only to an S-box component, never to the DNA layer.

The remainder of this paper is organized as follows. Section 2 fixes notation and states the working hypotheses. Sections 3–5 establish the three theorems. Section 6 analyzes the chained designs and presents the replacement. Section 7 reports the experimental and corpus results. Section 8 delimits the scope of the claims, and Section 9 concludes.

2 Preliminaries and notation

2.1 Notation

Throughout the paper, the symbols of Table 1 are used. Vectors over $\mathbb{F}_2$ are written as column vectors, and $\oplus$ denotes addition in $\mathbb{F}_2^m$, i.e. the bitwise exclusive-or.

2.2 DNA coding of images

In DNA-based image encryption, each 8-bit pixel is split into four 2-bit groups, and each group is mapped to one of the four nucleotide bases A, C, G, T. A grayscale image of $M \times N$ pixels thus becomes a sequence of $4MN$ symbols over Σ . An *encoding rule* is a bijection between the four 2-bit values and the four bases; there are

Table 1 Notation used throughout the paper.

Symbol	Meaning
Σ	the DNA alphabet $\{A, C, G, T\}$, $ \Sigma = 4$
ι	the fixed identification $\Sigma \rightarrow \mathbb{F}_2^2$ of Section 2.2
E_p, D_q	DNA encoding and decoding rules, $p, q \in \{1, \dots, 8\}$
$\odot$	a binary diffusion operation on Σ
κ	a key symbol, independent of the plaintext
$\deg F$	the algebraic degree of F (Definition 1)
$\text{GL}(m, 2)$	the group of invertible $m \times m$ matrices over $\mathbb{F}_2$
$\text{AGL}(m, 2)$	the affine group $\{x \mapsto Ax \oplus b : A \in \text{GL}(m, 2), b \in \mathbb{F}_2^m\}$
$\text{Sym}(\Sigma)$	the group of all bijections of Σ
$\text{DU}(F)$	the differential uniformity of F
$\text{NL}(F)$	the nonlinearity of F

$4! = 24$ such bijections, of which exactly eight respect the Watson–Crick complementarity constraint—a count stated routinely in this literature before the eight rules are selected [1–4]. The eight rules are used both to encode (pixels to bases) and, possibly with a different rule index, to decode (bases to pixels); dynamic schemes draw the rule index for each position or block from a chaotic sequence.

Diffusion is then performed at the symbol level: an encoded plaintext symbol is combined with a key symbol—produced by a chaotic generator—through a binary operation $\odot$ on Σ , specified by a 4×4 table. The operations in actual use are DNA addition and subtraction (the cyclic group $\mathbb{Z}_4$ under a chosen labeling of the bases), DNA XOR, and DNA XNOR [8].

We fix once and for all the identification $\iota : \Sigma \rightarrow \mathbb{F}_2^2$ given by $A \mapsto 00$, $C \mapsto 01$, $G \mapsto 10$, $T \mapsto 11$, and, through ι , treat every map on Σ as a map on $\mathbb{F}_2^2$. Nothing in Sections 3 and 4 depends on this choice; the reason is itself a consequence of Theorem 1 and is recorded in Remark 3.

2.3 Algebraic degree

Every Boolean function $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ has a unique representation as a multivariate polynomial over $\mathbb{F}_2$, the algebraic normal form (ANF) [22]; the degree of that polynomial is the *algebraic degree* of f .

Definition 1 Let $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ with coordinate functions $f_1, \dots, f_m$. The algebraic degree of F is $\deg F = \max_{1 \leq i \leq m} \deg f_i$, where $\deg f_i$ is the degree of the ANF of f_i .

Since $\deg(f \oplus g) \leq \max(\deg f, \deg g)$, the maximum over coordinate functions coincides with the maximum over all nonzero component functions $v \cdot F$, so Definition 1 agrees with the convention used for vectorial Boolean functions. A map has degree at most 1 precisely when it is *affine*, i.e. of the form $x \mapsto Ax \oplus b$; degree 1 maps compose to degree 1 maps, a fact used repeatedly below.

The relevance of the degree is classical: a cipher whose plaintext-to-ciphertext map is affine is broken by elementary linear algebra from a small number of known

or chosen plaintexts, regardless of its key length [15], and a low degree more generally bounds the resistance offered against algebraic [23] and higher-order differential [24] attacks. Degree is a necessary indicator, not a sufficient one—a point we return to in Section 8.

2.4 Working hypotheses

The results of Sections 3–5 are stated under the following hypotheses, each of which reflects the published constructions rather than a modeling convenience.

(A1) *Four-symbol alphabet.* The layer operates on Σ with $|\Sigma| = 4$, identified with $\mathbb{F}_2^2$ through ι . This is the defining choice of DNA coding.

(A2) *Symbol-wise operation.* The diffusion operation is given by a 4×4 table applied base by base. Every operation table published in the corpus surveyed in Section 7.5 is of this form; an operation acting on a coarser alphabet (e.g. a whole pixel at once) falls outside the scope of our results, a point made explicit in Section 8.

(A3) *Invertibility in the first argument.* For every fixed second operand b , the map $a \mapsto a \odot b$ is a bijection of Σ . Without (A3) the ciphertext symbol cannot be inverted during decryption, so (A3) is the minimum that any decryptable diffusion step must satisfy.

(A4) *Balance in the second argument* (used from Section 4 onward, where the second operand carries plaintext). For every fixed a , the map $b \mapsto a \odot b$ takes all four values. If (A4) fails for some symbol a , the previous-block operand cannot move the ciphertext of a through the full alphabet: the ciphertext of that symbol is confined to a proper subset of Σ whatever the chain carries, an imbalance visible in the ciphertext histogram and exhibited by two chosen plaintexts. (A4) is therefore imposed by the diffusion goal of the chaining itself.

Hypotheses (A1) and (A3) are in force throughout; (A2) delimits the object of study; (A4) is invoked only where stated.

3 Every keyed DNA operation is affine

The question addressed in this section is elementary to pose: the designer of a DNA diffusion layer is free to choose the operation table, the encoding and decoding rules, and their schedules—what algebraic degrees can the resulting keyed step $x \mapsto D_q(E_p(x) \odot \kappa)$ attain? The answer is that no choice attains more than degree one.

Theorem 1 *Let $\odot$ be any binary operation on Σ satisfying (A1) and (A3). Then for every key symbol $\kappa \in \Sigma$, the map $\sigma_\kappa : x \mapsto x \odot \kappa$ satisfies*

$$\deg \sigma_\kappa = 1;$$

that is, there exist $A \in \text{GL}(2, 2)$ and $b \in \mathbb{F}_2^2$ with $x \odot \kappa = Ax \oplus b$ for all $x \in \Sigma$.

Proof By (A3), σ_κ is a bijection of Σ , hence an element of $\text{Sym}(\Sigma)$, a group of order $4! = 24$. On the other hand, $|\text{GL}(2, 2)| = 6$, so

$$|\text{AGL}(2, 2)| = |\text{GL}(2, 2)| \cdot |\mathbb{F}_2^2| = 6 \cdot 4 = 24.$$

Every affine map with invertible linear part is a bijection of $\mathbb{F}_2^2$, so $\text{AGL}(2, 2) \leq \text{Sym}(\Sigma)$; since the two groups have the same finite order, they are equal. Hence $\sigma_\kappa \in \text{AGL}(2, 2)$, so $\deg \sigma_\kappa \leq 1$; and $\deg \sigma_\kappa \geq 1$ because a constant map is not a bijection. $\square$

Remark 1 The proof is elementary, and we do not present it as deep mathematics. The observation we wish to make is of a different kind: a literature that has stated the count $4! = 24$ paper after paper—as the number of available encoding rules; twenty-four times in the corpus of Section 7.5 alone—has not, in fifteen years of designs and cryptanalyses, read this number as the order of an affine group. Read that way, it forecloses the entire design space at once. The set of operations satisfying (A3) contains $24^4 = 331,776$ elements (an independent column permutation for each key symbol); Theorem 1 covers all of them, and an exhaustive enumeration in the accompanying repository confirms that every one of the 331,776 operations is affine for every key, with no exception.

3.1 Consequences for the full layer

Corollary 2 *Under (A1)–(A3), the complete diffusion step $x \mapsto D_q(E_p(x) \odot \kappa)$ is affine for every choice of encoding rule E_p , decoding rule D_q , operation $\odot$, and key κ .*

Proof E_p and D_q are bijections of Σ , hence affine by Theorem 1; σ_κ is affine; and the composition of affine maps is affine: $A_2(A_1x \oplus b_1) \oplus b_2 = (A_2A_1)x \oplus (A_2b_1 \oplus b_2)$. $\square$

Corollary 3 *No iteration count and no key schedule escapes Corollary 2: any number of rounds of keyed DNA steps, with arbitrary (possibly key-dependent) rule and operation schedules, composes affine maps and therefore remains affine. Consequently, the layer acting on a sequence of n symbols is an affine map of $\mathbb{F}_2^{2n}$, namely $y = Ax \oplus b$ with A a product of block-diagonal matrices (one $\text{GL}(2, 2)$ block per symbol) and permutation matrices.*

Remark 2 (Plaintext-dependent schedules) Many schemes make the rule indices themselves depend on the plaintext, either through the symbol value or through a hash of the whole image that seeds the chaotic generator. Neither mechanism raises the degree. If the rule index is a function of the symbol being encrypted, the resulting map of Σ is still a bijection—decryption requires it—and Theorem 1 applies to the assembled map exactly as to its parts; an exhaustive check over all 8^4 symbol-dependent selectors, 8 decoding rules and 4 keys finds a maximal degree of 1. If instead the schedule is derived from an image hash, then within any single encryption the schedule is a constant, so the layer is affine for that image; hash seeding varies the affine map *between* images, which obstructs naive multi-image attacks but contributes no nonlinearity to any single encryption. We return to the quantitative consequences of this mechanism in Section 7.

Remark 3 (The degree is canonical precisely here) The algebraic degree of a map on an alphabet is defined relative to an identification of the alphabet with $\mathbb{F}_2^m$. For $|\Sigma| = 4$ the choice does not matter: any two identifications differ by a bijection of Σ , which is itself affine by Theorem 1, and conjugating by affine maps preserves the degree [25]. On larger alphabets this fails—the same operation can exhibit different degrees under different labelings—so the

degree is a canonical invariant of the operation exactly in the case $m \leq 2$ that DNA coding occupies. The same phenomenon reappears from the opposite direction in Section 5.

3.2 Published analyses as special cases

Several published cryptanalyses of DNA-based schemes establish, for one scheme at a time, algebraic collapses that Theorem 1 yields uniformly. Two are representative.

Proposition 4 (Codec collapse; cf. [4]) *Consider the eight Watson–Crick rules with their standard numbering, used once to encode and once to decode. All 64 compositions $D_q \circ E_p$ are affine, and exactly eight of them equal the bitwise complement $x \mapsto x \oplus 11$, namely those with $p + q = 9$.*

The affinity of all 64 pairs is immediate from Theorem 1; the identification of the complementary pairs $p + q = 9$ recovers, by direct computation, the codec identity on which the nine-plaintext attack of Wen et al. [4] is built.

Belazi et al. [13] prove, for the scheme of [12], that DNA addition performed after encoding is equivalent to a single binary addition, independently of the encoding rule—their “first equivalence”. Computation shows this equivalence to be a property of the particular encoding family involved: conjugating the $\mathbb{Z}_4$ addition table by an arbitrary encoding returns $\mathbb{Z}_4$ addition for only 2 of the 24 encodings (and preserves XOR for 6 of 24). Theorem 1 requires no such compatibility: whether or not the conjugated operation retains the group structure, it is a keyed bijection of a four-letter alphabet and therefore affine. The scheme-specific collapses of [4, 13, 14] are, in this sense, instances of a single structural fact.

Remark 4 (Attack cost, and what is not claimed) Theorem 1 does not yield a new attack, and we claim none. A generic affine map of $\mathbb{F}_2^{2n}$ would require $2n + 1$ chosen plaintexts to identify—over half a million for a 256×256 image—but the layer of Corollary 3 is far from generic: it carries one of 24 bijections per symbol and one position permutation, about $n \log_2 24 + \log_2 n!$ secret bits in total, so information-theoretically on the order of a dozen chosen plaintexts suffice (11 for 256×256). Published attacks already operate at this scale—nine chosen plaintexts in [4]. What the theorem adds is not a better attack but an explanation and an inevitability: affinity is not a defect of the particular schemes that were broken, it is a property of the design space, and no operation table, encoding schedule, or round count within that space could have prevented any of these attacks.

4 Two plaintext-dependent operands: the ceiling

Theorem 1 leaves exactly one escape route inside the four-letter alphabet: since any operation with a single plaintext-dependent operand is affine, a nonlinear step must take *two* operands that vary with the plaintext. This is precisely the shape of the chained constructions that have recently appeared, in which the current sub-block is combined with the *previous* sub-block rather than with a key symbol alone (Section 6). The present section determines what this escape route can and cannot deliver.

4.1 The admissible class

When both operands carry plaintext, hypothesis (A3) is still forced by decryption, and hypothesis (A4) is forced by the purpose of the chaining: a symbol whose row is unbalanced ignores part of the chain, which is a distinguisher observable from two chosen plaintexts. Together the two hypotheses say that every row and every column of the operation table is a permutation of Σ :

Proposition 5 *An operation on Σ satisfies (A3) and (A4) if and only if its table is a Latin square of order 4. There are exactly 576 such operations.*

The count is classical, and an enumeration of the 331,776 operations satisfying (A3) confirms that exactly 576 survive (A4). All four operations in actual use—DNA addition, subtraction, XOR and XNOR—belong to this class. Order-four quasigroups, and their partition into 144 linear and 432 nonlinear operations, are known objects in quasigroup-based cryptography [26, 27]; there the very weakness of a single order-four quasigroup is the reason such designs *compose* several of them. Our contribution below is not this partition but the fact that differential uniformity and nonlinearity are pinned at their worst values across *all* 576 operations, and its structural cause in the alphabet size (Proposition 7).

For the statement of the next theorem we recall the two standard indicators beyond the degree [28]. For $F : \mathbb{F}_2^4 \rightarrow \mathbb{F}_2^2$ (the operation as a map of both operands), the *differential uniformity* [29] is $\text{DU}(F) = \max_{d \neq 0} \max_c \#\{x : F(x) \oplus F(x \oplus d) = c\}$, for which the attainable range here is $4 \leq \text{DU}(F) \leq 16$; and the *nonlinearity* $\text{NL}(F)$ is the minimum Hamming distance from a nonzero component function of F to the affine Boolean functions [30, 31], with maximum attainable value 6 for this shape. Both indicators carry their standard operational meaning: a differential uniformity of DU caps the probability of any single differential at $\text{DU}/2^4$, and it is against that bound that provable resistance to differential cryptanalysis is stated [32].

4.2 The ceiling

Theorem 6 *Let $\odot$ satisfy (A1), (A3) and (A4), and view it as a map $F : \mathbb{F}_2^2 \times \mathbb{F}_2^2 \rightarrow \mathbb{F}_2^2$ of both operands. Then:*

- (a) $\deg F \leq 2$. The bound is attained by exactly 432 of the 576 admissible operations.
- (b) The remaining 144 operations have degree 1, and they are exactly the operations of the form $a \odot b = M_1 a \oplus M_2 b \oplus c$ with $M_1, M_2 \in \text{GL}(2, 2)$ and $c \in \mathbb{F}_2^2$; the count is $|\text{GL}(2, 2)|^2 \cdot 4 = 144$. DNA XOR and XNOR belong to this class; DNA addition and subtraction attain degree 2.
- (c) For every one of the 576 admissible operations,

$$\text{DU}(F) = 16 \quad \text{and} \quad \text{NL}(F) = 0.$$

Parts (a) and (c) are not accidents of the operations in use; they follow structurally from the same fact that drives Theorem 1, and the mechanism locates the weakness in the alphabet size rather than in any choice of operation.

Proposition 7 *Let $\odot$ be a Latin square on $\Sigma \cong \mathbb{F}_2^2$ and let $F(a, b) = a \odot b$, viewed as a map $\mathbb{F}_2^2 \times \mathbb{F}_2^2 \rightarrow \mathbb{F}_2^2$.*

- (i) *F is biaffine: $F(a, b) = M(a, b) \oplus L_1(a) \oplus L_2(b) \oplus c$ with M a $\mathbb{F}_2$ -bilinear vectorial map and L_1, L_2 linear. Hence $\deg F \leq 2$, with $\deg F = 2$ iff $M \neq 0$.*
- (ii) *For every mask $v \in \mathbb{F}_2^2 \setminus \{0\}$ the component bilinear form $\langle v, M \rangle$, written $a^\top N_v b$, has $\text{rank } N_v \leq 1$.*

Consequently $\text{NL}(F) = 0$ and $\text{DU}(F) = 16$.

Proof (i) For each fixed b the column map $a \mapsto a \odot b$ is a bijection of Σ , hence affine by Theorem 1. Thus F is affine in a for every fixed b and, symmetrically, affine in b for every fixed a . The mixed second difference $M(a, b) := F(a, b) \oplus F(a, 0) \oplus F(0, b) \oplus F(0, 0)$ is then $\mathbb{F}_2$ -bilinear and $F \oplus M$ is affine. The only quadratic monomials of a bilinear form are the mixed products $a_i b_j$, so $\deg F \leq 2$, with a genuine quadratic term present iff $M \neq 0$.

(ii) Fix $v \neq 0$ and write $\langle v, F(a, b) \rangle = a^\top N_v b \oplus w^\top a \oplus r(b)$. For each fixed b , the map $a \mapsto \langle v, F(a, b) \rangle$ is a coordinate of the bijection $F(\cdot, b)$, hence balanced. An affine Boolean function is balanced iff its linear part is nonzero, so the coefficient $N_v b \oplus w$ must be nonzero for every b ; equivalently $w \notin \text{Im } N_v$. If $\text{rank } N_v = 2$ then $\text{Im } N_v = \mathbb{F}_2^2 \ni w$, a contradiction. Hence $\text{rank } N_v \leq 1$.

For $\text{NL}(F) = 0$ it suffices that one nonzero component of F be affine, i.e. that one of the three forms $N_{e_1}, N_{e_2}, N_{e_1} \oplus N_{e_2}$ vanish. Suppose none does; then all three are nonzero and, by (ii), of rank exactly 1. A sum of two distinct nonzero rank-1 matrices over $\mathbb{F}_2$ has $\text{rank} \leq 1$ only when the summands share a left or a right factor; transposing to the row map if it is the latter, we may write $N_{e_k} = u v_k^\top$ with a common $u \neq 0$ and $v_1 \neq v_2$. Then $M(a, b) = (u^\top a) V b$ with $V = [v_1^\top; v_2^\top] \in \text{GL}(2, 2)$, so the linear part of the column map $a \mapsto F(a, b)$ is $C(b) = L_1 \oplus (V b) u^\top$, where $L_1 = C(0) \in \text{GL}(2, 2)$. By the rank-one determinant identity $\det(I \oplus x y^\top) = 1 \oplus y^\top x$,

$$\det C(b) = \det L_1 \cdot (1 \oplus u^\top L_1^{-1} V b),$$

which is 0 for any b with $u^\top L_1^{-1} V b = 1$; such a b exists because $u^\top L_1^{-1} V \neq 0$, contradicting $C(b) \in \text{GL}(2, 2)$. Hence some component vanishes and $\text{NL}(F) = 0$. Finally, for biaffine F the derivative $D_\alpha F(a, b) = M(\alpha_a, b) \oplus M(a, \alpha_b) \oplus \text{const}$ is constant exactly when α_a and α_b lie in the left and right radicals of M ; a nonzero rank-1 form has a one-dimensional radical on each side, so a nonzero linear structure α exists, giving a dead difference and $\text{DU}(F) = 16$. If $M = 0$ then F is affine and all 15 nonzero differences are dead. $\square$

Proposition 7 reduces Theorem 6 to the alphabet size: biaffinity is exactly Theorem 1 (the $m \leq 2$ regime of Theorem 8) applied in each operand, and the rank collapse it forces is what pins DU and NL at their worst values. The degree split—432 operations at degree 2 and 144 at degree 1, matching Theorem 6(b)—together with $\text{DU} = 16$ and $\text{NL} = 0$ throughout is confirmed by exhaustive computation over

the 576 operations, with each indicator evaluated by two independent implementations (repository); this serves as corroboration rather than proof. Two aspects of the statement deserve emphasis.

First, $\text{DU}(F) = 16$ is the *ceiling*, not the floor: it asserts the existence of a nonzero input difference under which all 16 input pairs produce one and the same output difference—a completely dead difference. The refined count is that each of the 432 degree-2 operations has exactly 3 dead differences among the 15 nonzero ones, while each of the 144 affine operations has all 15. For DNA addition the dead difference is visible by hand: with $\Delta = (2, 2)$,

$$(a + 2) + (b + 2) \equiv a + b \pmod{4},$$

so the output difference vanishes for every input. The conclusion is unchanged if the attacker is restricted to differences in the first operand only, so it does not depend on the threat model.

Second, the ceiling survives the structure actually used in the chained designs, where the key is folded in before the chaining step: enumerating maps of the form $(p, c_{\text{prev}}) \mapsto (p \odot_1 \kappa) \odot_2 c_{\text{prev}}$ over admissible $\odot_1, \odot_2$ and all keys again yields no degree above 2.

Remark 5 (A degree-3 mirage) If (A4) is dropped, the picture changes sharply: among the 331,776 operations satisfying (A3) alone, 92.6% reach degree 3, and one may hope to use them. The hope is empty. Every degree-3 operation in that class has at least one unbalanced row, i.e. a plaintext symbol whose ciphertext is confined to a proper subset of Σ regardless of the second operand—the distinguisher that motivated (A4) in the first place. Once the chaining is required to diffuse, the admissible class is the 576 Latin squares and the ceiling is 2.

Table 2 The four operations in published use, as maps of two plaintext-dependent operands. All satisfy (A1), (A3), (A4).

Operation	deg (keyed operand)	deg (both free)	DU	NL
DNA addition ($\mathbb{Z}_4$)	1	2	16	0
DNA subtraction ($\mathbb{Z}_4$)	1	2	16	0
DNA XOR	1	1	16	0
DNA XNOR	1	1	16	0
best admissible operation	1	2	16	0

4.3 What the escape route buys

Theorem 6 is a half-open door. Moving from one plaintext-dependent operand to two raises the attainable degree from 1 to 2—and that is all it does. Differential uniformity

and nonlinearity are pinned at their worst possible values for every admissible operation on the four-letter alphabet, including the best one (Table 2): no choice of operation can improve either indicator. The design consequence is developed in Section 6; the structural reason—that the obstruction belongs to the alphabet size rather than to the operations—is the subject of the next section.

5 Why four letters: the alphabet-size boundary

The two preceding sections could be read as statements about DNA operations. They are not: they are statements about the number four. To make this precise, let Σ_m denote an alphabet of 2^m symbols identified with $\mathbb{F}_2^m$, so that DNA coding is the case $m = 2$.

Theorem 8 *$\text{AGL}(m, 2) = \text{Sym}(\Sigma_m)$ if and only if $m \leq 2$. Consequently, the impossibility of Theorem 1—that every keyed symbol map is affine—holds for $m \leq 2$ and fails for every $m \geq 3$.*

Proof For $m \leq 2$ the two orders agree: $|\text{AGL}(1, 2)| = 2 = 2!$ and $|\text{AGL}(2, 2)| = 24 = 4!$; since $\text{AGL}(m, 2) \leq \text{Sym}(\Sigma_m)$ always holds, equality of orders gives equality of groups. For the converse it suffices to show $|\text{AGL}(m, 2)| < (2^m)!$ for all $m \geq 3$. Each of the m factors of $|\text{GL}(m, 2)| = \prod_{i=0}^{m-1} (2^m - 2^i)$ is smaller than 2^m , so

$$|\text{AGL}(m, 2)| < 2^m \cdot (2^m)^m = 2^{m(m+1)}.$$

Passing from m to $m + 1$ multiplies this bound by 2^{2m+2} , while $(2^m)!$ grows to $(2^{m+1})! \geq ((2^m)!) \cdot (2^m)^{2^m} = ((2^m)!) \cdot 2^{m2^m}$, and $m2^m > 2m + 2$ for every $m \geq 2$. Since the factorial already exceeds the bound at $m = 3$ ($8! = 40,320 > 2^{12} = 4,096$; indeed $|\text{AGL}(3, 2)| = 1,344 < 40,320$), it never loses the lead. $\square$

The fraction of bijections that are affine collapses immediately beyond the boundary (Table 3): at $m = 3$ only one bijection in thirty is affine; at $m = 4$, one in sixty-five million. DNA coding sits exactly at the edge:

Corollary 9 *The DNA alphabet, with $4 = 2^2$ symbols, is the largest alphabet for which the impossibility of Theorem 1 applies. On any larger power-of-two alphabet, keyed non-affine substitutions exist in abundance.*

It bears repeating that the alphabet size was never a cryptographic decision. Four bases were adopted from the biological metaphor, and the count $4! = 24$ has been restated in this literature for fifteen years as an inventory of encoding options. Theorem 8 identifies the same number as the order of $\text{AGL}(2, 2)$, and with it the reason no operation table on this alphabet was ever going to be nonlinear.

Table 3 The fraction of alphabet bijections that are affine, $|\text{AGL}(m, 2)|/(2^m)!$.

m	alphabet size	$ \text{AGL}(m, 2) $	affine fraction
1	2	2	1
2	4	24	1
3	8	1,344	3.3×10^{-2}
4	16	322,560	1.5×10^{-8}
5	32	3.2×10^8	1.2×10^{-27}
6	64	1.3×10^{12}	1.0×10^{-77}

5.1 What a larger alphabet buys: an observation

Theorem 8 says only that the *obstruction* disappears at $m = 3$; it does not say that an eight-letter layer is secure. At $m = 4$ the corresponding question has been settled by exhaustive classification of the 4-bit bijections into affine-equivalence classes [33]; no census of that kind is attempted here. To gauge what becomes available, order-8 quasigroups (the analogue of the admissible class of Proposition 5) were sampled at random and their indicators computed under the natural identification of $\{0, \dots, 7\}$ with $\mathbb{F}_2^3$.

Observation 1 Over a sample of 60 random Latin squares of order 8, the best profile found was algebraic degree 4, $\text{DU} = 20$ out of a ceiling of 64 (31%), and $\text{NL} = 20$ out of a maximum of 28 (71%). For comparison, the four-letter class of Theorem 6 is pinned, in its entirety, at 100% of the DU ceiling and 0% of the attainable NL.

Three caveats bound this observation, and it is offered as nothing more. First, at $m \geq 3$ the algebraic degree is no longer independent of the identification of the alphabet with $\mathbb{F}_2^m$ —the same operation can exhibit different degrees under different labelings (for $m = 2$ this cannot happen, by Remark 3)—so the degree figure is tied to the stated identification. Second, the sample is a random draw, not a search or an enumeration: the figures are a lower bound on what a directed construction could achieve. Third, nothing here bounds an attacker; the comparison measures only what the designer is no longer prevented from building. Extended DNA models with more than four bases have already begun to appear in this literature [7], so the boundary of Theorem 8 is not of purely theoretical interest.

6 Chained DNA diffusion in recent designs

The escape route of Section 4 is not hypothetical. Four recent papers—three journal articles from 2024 and one conference paper from 2023 [18–21]—independently adopt the same construction: the image is split into sub-blocks, and after the keyed DNA operation, *the result of the current sub-block is combined, by a second DNA operation, with the previous sub-block*. In the words of [18]: “for a better diffusion effect, the encryption result of the current sub-block is again subjected to DNA operation with

the previous sub-block (except for the first sub-block)”; the formulations in [19–21] are equivalent.¹ This is exactly the two-plaintext-operand shape that Theorem 6 analyzes, and all four papers motivate it purely as diffusion; none reports an algebraic indicator of any kind.

In all four schemes the operation applied at each step is drawn from the four-item menu

$$Z_i = 0 \mapsto \text{addition}, \quad Z_i = 1 \mapsto \text{subtraction}, \quad Z_i = 2 \mapsto \text{XOR}, \quad Z_i = 3 \mapsto \text{XNOR},$$

where $\{Z_i\}$ is an unconstrained chaotic sequence. The addition tables printed in the four papers were transcribed and tested: all four are the cyclic group $\mathbb{Z}_4$ under a labeling of the bases (the labelings differ between papers, which by Remark 3 changes nothing), and are in particular *associative*. The analysis below therefore applies to the schemes as published, not to a reconstruction of them.

6.1 Half the menu is affine

By Theorem 6, addition and subtraction reach degree 2, while XOR and XNOR belong to the 144 operations that remain affine in both operands. With $\{Z_i\}$ effectively uniform, each chaining step is left affine with probability $1/2$: in an image of n sub-blocks, the expected number of steps contributing no nonlinearity at all is $n/2$, and the probability that every step reaches degree 2 is 2^{-n} —about 5×10^{-20} already for $n = 64$. The algebraic degree of the layer is thus left to chance, block by block, unmeasured and unreported.

6.2 The associative collapse

Restricting the menu to $\{\text{addition, subtraction}\}$ removes the affine entries at no cost. It does not, however, make the chain benefit from its length, and the reason is associativity. Writing the chained layer over one symbol position as $c_k = p_k \odot c_{k-1}$, associativity of $\mathbb{Z}_4$ addition unrolls the chain into a single prefix sum $c_k = p_1 + p_2 + \dots + p_k + \text{const} \pmod{4}$: however long the chain, the map is one modular sum, whose high bit is the elementary symmetric polynomial of degree 2.

Both consequences were measured on the full chain map $(p_1, \dots, p_k) \mapsto (c_1, \dots, c_k)$, a bijection of $\mathbb{F}_2^{2k}$. First, the algebraic degree of the $\mathbb{Z}_4$ chain is pinned: it equals 2 for every chain length tested ($k \leq 7$). Second, and more damaging, the chain *accumulates linear structures*—nonzero differences d for which $F(x) \oplus F(x \oplus d)$ is the same for every x [34]. For the $\mathbb{Z}_4$ chain their number is $2^k - 1$ (verified exhaustively for $k \leq 6$), growing with the length of the chain; each is an image-independent differential of exactly the kind exhibited experimentally in Section 7. For XOR chaining, every difference is a linear structure—the layer is entirely linear.

¹Reference [20] names the four operations addition, subtraction, “heteroscedasticity” and “homoscedasticity” of DNA; its printed tables identify the latter two as DNA XOR and XNOR.

6.3 A zero-cost replacement

Associativity, however, is a property of the chosen operation, not of the construction. Among the 432 degree-2 operations of Theorem 6, exactly 288 make the chain degree *grow* with its length; none of them is associative, and every associative operation lies in the 144 that stay pinned (non-associativity alone is not sufficient: 132 non-associative operations also stay pinned). One representative, written in the base alphabet with the identification ι of Section 2.2, is

$$\begin{array}{c|cccc} \odot & A & C & G & T \\ \hline A & A & C & T & G \\ C & C & G & A & T \\ G & G & T & C & A \\ T & T & A & G & C \end{array} \quad (1)$$

This table is a Latin square, so it satisfies (A3) and (A4) and decrypts by the same column-inverse lookup as $\mathbb{Z}_4$ subtraction; a round trip over 20,000 random chains of random lengths confirms exact decryption. Replacing the menu by the single operation (1)—same 4×4 table size, same invertibility, same decryption cost—changes the two measured quantities as follows: the degree of the full chain map becomes k for chains of length k (Fig. 1a) (measured through $k = 9$, against the constant 2 of $\mathbb{Z}_4$), and the number of linear structures is *constant at 3* for every chain length tested, against $2^k - 1$ (Fig. 1b). The three surviving structures are the dead differences of the single operation (Theorem 6); the chain adds none.

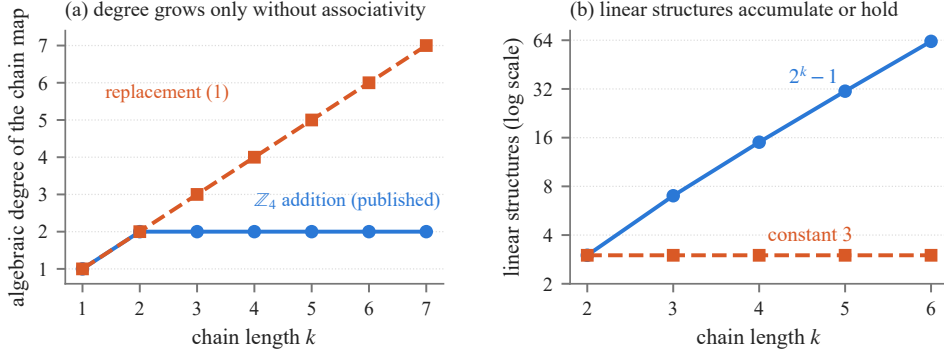


Fig. 1 The chained layer, $\mathbb{Z}_4$ addition (as published) against the replacement (1), measured on the full chain map $(p_1, \dots, p_k) \mapsto (c_1, \dots, c_k)$: (a) algebraic degree; (b) number of linear structures.

6.4 Improved, not repaired

The recommendation that follows is modest. Dropping XOR and XNOR from the menu costs nothing and stops the layer’s degree from being left to chance; replacing the menu by a non-associative degree-2 operation such as (1) additionally makes the chain degree grow with its length and stops the accumulation of linear structures. Neither change touches part (c) of Theorem 6: differential uniformity and nonlinearity remain at their worst possible values, as they do for every admissible operation on four letters. The construction is *improved, not repaired*; on this alphabet, by Corollary 9, repair is not available.

7 Experimental validation

The claims of Sections 4 and 6 concern what the standard evaluation methodology can and cannot see. This section makes that concrete on a faithful implementation of the chained layer of Section 6: dynamic Watson–Crick encoding per chunk, a keyed DNA operation, and chaining with the previous chunk, with all schedule material drawn from a logistic keystream. Three variants share every line of the implementation except the operation menu: **published** uses the four-item menu of [18–21]; **restricted** uses {addition, subtraction}; and **replacement** uses the single operation (1). Test images are four 256×256 medical images (chest radiographs, an MR slice and a CT scout view) and the Lena reference image; exact round-trip decryption was verified for every encryption reported below.

7.1 The standard battery does not separate the variants

Table 4 reports the battery that the four papers—and this literature generally—use to argue security: ciphertext entropy, histogram χ^2 , adjacent-pixel correlation, and the plaintext sensitivity scores NPCR and UACI [9], under the image-hash seeding that all four schemes employ. Every figure is in the range this literature reports as ideal, and the three variants are statistically indistinguishable on every line. A reviewer shown this table alone—the table these papers publish—has no means of telling the three apart, although one of them contains affine chaining steps with probability $1/2$ per block and another provably accumulates none. This is the depreciation of statistical evidence observed in general by [35], here exhibited within a single construction.

Table 4 Mean values over the five test images, image-hash seeding as published. NPCR/UACI in %, one-bit plaintext change.

Variant	Entropy	χ^2	NPCR	UACI
published	7.9970	274.5	99.60	33.50
restricted	7.9971	263.3	99.60	33.43
replacement	7.9970	273.6	99.60	33.48

7.2 Where the reported avalanche comes from

The near-ideal NPCR of Table 4 is produced by the key schedule, not by the DNA layer. All four schemes derive the chaotic seeds from a hash of the plaintext image, so a one-bit change replaces the entire keystream. When the seed is held fixed—the only way to measure the layer’s own diffusion—the NPCR of all three variants collapses to 0.195% (Fig. 2): the chaining is element-wise between consecutive chunks, so a change at position i reaches position i of subsequent chunks and nowhere else. The avalanche these papers report is the work of the hash, not of the step they motivate as “diffusion”; within a fixed-key encryption the layer is exactly as weak as Corollary 3 and Section 6.2 describe, and the hash seeding conceals this from the battery (cf. Remark 2).

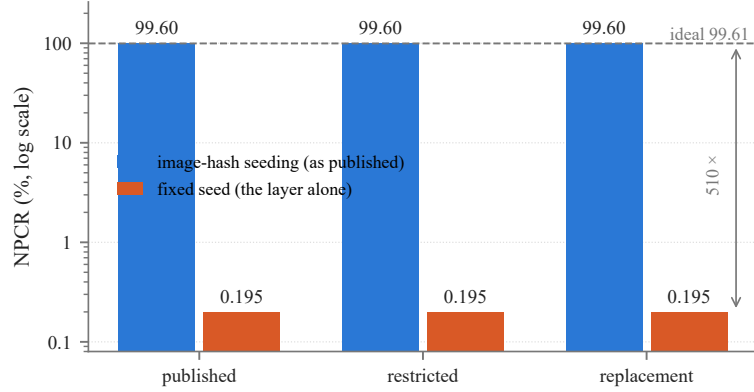


Fig. 2 Where the reported avalanche comes from. Mean NPCR, on a logarithmic axis, for the three variants under the image-hash seeding used by the published schemes (five test images) and under a fixed seed (the three medical images, for which the value is identical). The near-ideal figure belongs to the re-seeding mechanism; the layer itself moves 0.195% of the pixels, a factor of 510 smaller.

7.3 The image-independent differential

The linear structures of Section 6.2 are observable on real images. With the encoding rule and key fixed, the difference $\Delta = +2 \pmod{4}$ applied to one symbol—the order-2 element of $\mathbb{Z}_4$, i.e. the dead difference of Theorem 6—was injected at two positions of a chain of $k = 8$ symbols, over 400 windows drawn at random from the five test images. For $\mathbb{Z}_4$ chaining the resulting ciphertext difference pattern is *identical in every window of every image*: an attacker measures it once, on an image of his choosing, and it holds everywhere. The differences $+1$ and $+3$ produce many patterns, as does every tested difference under the replacement operation (1): 2 of the 6 tested (position, difference) pairs are image-independent for the published operation, 0 of 6 for the replacement. No line of Table 4 carries any trace of this distinction.

7.4 The certificate applied to the published operations

The distinction the battery misses is, by contrast, immediate to the certificate. Table 5 reports it for the whole operation set in published use—DNA XOR and XNOR, and $\mathbb{Z}_4$ addition and subtraction—each obtained by Möbius enumeration of the operation table. Two things are legible at once that Table 4 cannot show. First, the operations are not interchangeable: XOR and XNOR are affine (degree 1) even when both operands carry plaintext, so a layer built on DNA-XOR is linear end to end and yields to linear algebra, whereas $\mathbb{Z}_4$ addition and subtraction reach the degree-2 ceiling. This is the very split that separates the schemes dismantled in [4, 13, 14] from the harder targets, and it is readable in the certificate before a single image is encrypted. Second, and uniformly, every published operation sits at $\text{DU} = 16$ and $\text{NL} = 0$: the weakness of Theorem 6 is a property of the whole published set, not of one poor choice within it.

Table 5 Certificate of the DNA operations in published use, in the keyed (one plaintext-dependent operand) and chained (two operands) regimes. Regenerated in the repository; by Theorem 1 the certificate is invariant under all 24 encodings, which is verified there.

Operation	deg keyed	deg chained	DU	NL	class
DNA XOR	1	1	16	0	affine
DNA XNOR	1	1	16	0	affine
$\mathbb{Z}_4$ addition	1	2	16	0	degree-2 ceiling
$\mathbb{Z}_4$ subtraction	1	2	16	0	degree-2 ceiling

That the certificate is independent of the encoding rule is itself a corollary of Theorem 1: an encoding is an affine bijection of Σ , so a change of encoding conjugates the operation by an affine map and leaves degree, differential uniformity and nonlinearity unchanged. A designer therefore need not fix an encoding to certify a layer—the three numbers are properties of the operation itself—and the entire audit of Table 5, four operations across both regimes and all 24 encodings, is produced by a single command in well under a second. This is the concrete form of the paper’s proposal: an encoding-agnostic certifier that takes any proposed DNA or chaining table and returns the row it would occupy above, at a cost negligible beside the statistical battery it would accompany.

7.5 The corpus measurement

Finally, the absence that motivates this paper was itself measured. A corpus of 154 distinct documents was assembled from three collections gathered for a doctoral literature review—122 of them papers proposing an image cipher of the chaotic or DNA family, the remainder reference works, textbooks and surveys of the same field. In the 122 design papers, the term *algebraic degree* occurs zero times; so do *differential uniformity* and *algebraic weakness*; the term *nonlinearity* appears in 26 of them, in every examined case applied to an S-box component and never to the DNA or chaining layer

of the same paper. In the reference works, by contrast, 70% carry this vocabulary—the knowledge is on the shelf, and does not reach the design table. Most telling of all, the count $4! = 24$ is stated 24 times, in 23 papers of the corpus, always as an inventory of encoding rules and never as the order of $\text{AGL}(2, 2)$; the file-and-page list is included in the repository. The corpus is a convenience sample, not a systematic review, and is offered with that limitation (Section 8); its uniformity is nonetheless difficult to attribute to sampling.

All figures in this section, and every enumeration in Sections 3–6, are regenerated by single commands from the accompanying repository, which also produces a machine-checked ledger of all 32 numerical claims.

8 Scope and limitations

What the theorems do and do not cover.

All results concern the symbol-wise layer delimited by hypothesis (A2): a 4×4 operation table applied base by base, which is the form of every operation table in the corpus examined. A substitution acting on a coarser unit—a whole pixel at once, i.e. a 256-letter alphabet—escapes Theorem 1 entirely, since $|\text{AGL}(8, 2)| \approx 1.4 \times 10^{21}$ against $256! \approx 8.6 \times 10^{506}$ bijections; by Theorem 8 this is a design direction, not a defect of the analysis. The results likewise say nothing about the permutation stage or the chaotic generator of any scheme: they bound one layer, the one that carries the name “DNA diffusion”.

Degree is necessary, not sufficient.

A layer of degree 1 admits a complete break by linear algebra, so degree ≥ 2 is a prerequisite; it is in no way a guarantee. The history of cellular-automata cryptography is the standing warning: stream ciphers built on the degree-2 rule 30 were broken by Meier and Staffelbach [36] through exactly the kind of structural analysis applied here. Accordingly, no security claim is made for the replacement operation of Section 6.3: it removes an identified affine fraction and a growing family of linear structures, while differential uniformity and nonlinearity remain at the values that Theorem 6 fixes for the whole class. The construction is improved, not repaired, and on four letters cannot be repaired.

The corpus.

The corpus of Section 7.5 was assembled for a doctoral literature review, not by a registered systematic search; the counts reported there are offered as a measurement of that corpus, with the obvious sampling caveat. Independent web searches conducted while preparing this paper found no design-side use of the algebraic degree for DNA layers either, but absence of evidence from a convenience sample is stated as such.

Larger alphabets.

Observation 1 rests on a random sample of 60 order-8 quasigroups and on one fixed identification of the alphabet with $\mathbb{F}_2^3$; at $m \geq 3$ the degree is identification-dependent, so the figures are indicative bounds, not invariants. Constructing and certifying a

concrete eight-letter DNA layer—where 96.7% of bijections are non-affine—is left as the natural continuation of this work.

9 Conclusions

The algebraic structure of DNA diffusion layers has been analyzed at the level of the design space rather than of individual schemes. Because the DNA alphabet has four letters, every bijection of it is affine over $\mathbb{F}_2$: consequently every decryptable keyed DNA operation—all 331,776 of them, under all 24 encoding rules, any schedule and any number of rounds—has algebraic degree 1 (Theorem 1). With two plaintext-dependent operands the degree can reach 2 and no more, and differential uniformity and nonlinearity are pinned at their worst possible values for every admissible operation (Theorem 6); four is the largest alphabet size for which this obstruction exists at all (Theorem 8). Applied to a chained construction adopted in four recent schemes, the analysis located two concrete defects—an operation menu half of which is affine, and an associative operation whose chain accumulates $2^k - 1$ linear structures—and a replacement operation of identical cost that removes both, verified end to end on medical images.

This differs from prior work on DNA-based ciphers in two ways. First, the published algebraic analyses [4, 13, 14] each dismantle one scheme; the theorems above show their common mechanism to be a property of the design space, of which those results are special cases, and explain why a decade of such attacks kept succeeding by near-identical means. Second, the output is design-side rather than attack-side: the algebraic degree of a proposed layer is computable in seconds by Möbius enumeration of its operation table, and the criteria involved—two plaintext-dependent operands, an operation outside the 144 bilinear-affine Latin squares, non-associativity if the chain is to gain from its length—are checkable by counting, before publication, and reportable as a number.

Three routes lead out of the impossibility, in increasing order of ambition: restrict or replace the operation menu within the four-letter alphabet, which is free and is the improvement recommended here; accept the ceiling of degree 2 that any four-letter chaining obeys; or leave the alphabet, where Theorem 8 shows the obstruction dissolve. Whichever route a designer takes, the experiments of Section 7 support one methodological conclusion: the statistical battery on which this literature rests cannot distinguish a layer that is affine half the time from one that never is, nor detect an image-independent differential that an attacker can measure once and use everywhere. The algebraic degree of the diffusion layer costs seconds to certify; the evaluation tables of this literature have room for one more number, and it is the one that would have exposed every break discussed in this paper before publication rather than after.

Statements and Declarations. Competing Interests. The authors have no competing interests to declare that are relevant to the content of this article.

Funding. The authors declare that no funds, grants, or other support were received during the preparation of this manuscript.

Data and Code Availability. All enumerations, exhaustive censuses and verification runs reported here are reproduced by the accompanying package; a ledger maps every numerical claim to the script that regenerates it, to its saved output, and to the command that reproduces it, and a single command regenerates the ledger of all 32 claims. The package is openly archived at Zenodo under doi:10.5281/zenodo.22774438, which resolves to <https://doi.org/10.5281/zenodo.22774438> and is openly accessible without registration. The medical test images of Section 7 are derived from the collection Pseudo-PHI-DICOM-Data of The Cancer Imaging Archive (TCIA), licensed CC BY 4.0. That collection is openly available without registration at the direct link <https://www.cancerimagingarchive.net/collection/pseudo-phi-dicom-data/> and carries the persistent identifier <https://doi.org/10.7937/s17z-r072> which resolves to the same page. As TCIA requires data citation, the collection is cited as: Rutherford, M., Mun, S.K., Levine, B., Bennett, W.C., Smith, K., Farmer, P., Jarosz, J., Wagner, U., Farahani, K., Prior, F. (2021). A DICOM dataset for evaluation of medical image de-identification (Pseudo-PHI-DICOM-Data) [Data set]. The Cancer Imaging Archive.

Author Contributions. Both authors (**Ihab Shakir**, I.S., and **Hossein Kheiri**, H.K.) are corresponding authors and contributed equally to the study conception and design. Theoretical conceptualization, methodology, and academic supervision were performed by **Hossein Kheiri** (H.K.). Mathematical modeling, formal algebraic proofs, computational implementation, exhaustive enumerations, and writing the original draft were carried out by **Ihab Shakir** (I.S.). Both authors (I.S. and H.K.) contributed to the analysis, critically reviewed and edited the manuscript, and approved the final version for publication.

Ethical Approval. Not applicable. This study did not involve human participants or animals.

References

- [1] Guesmi, R., Farah, M.A.B., Kachouri, A., Samet, M.: A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2. *Nonlinear Dynamics* **83**, 1123–1136 (2016) <https://doi.org/10.1007/s11071-015-2392-7>
- [2] Wang, X.-Y., Zhang, Y.-Q., Bao, X.-M.: A novel chaotic image encryption scheme using DNA sequence operations. *Optics and Lasers in Engineering* **73**, 53–61 (2015) <https://doi.org/10.1016/j.optlaseng.2015.03.022>
- [3] Zhang, Y., Xiao, D., Wen, W., Wong, K.-W.: On the security of symmetric ciphers based on DNA coding. *Information Sciences* **289**, 254–261 (2014) <https://doi.org/10.1016/j.ins.2014.08.005>
- [4] Wen, H., Yu, S., Lü, J.: Breaking an image encryption algorithm based on DNA encoding and spatiotemporal chaos. *Entropy* **21**(3), 246 (2019) <https://doi.org/10.3390/e21030246>

- [5] Khan, J.S., Boulila, W., Ahmad, J., Rubaiee, S., Rehman, A.U., Alroobaea, R., Buchanan, W.J.: DNA and plaintext dependent chaotic visual selective image encryption. *IEEE Access* **8**, 159732–159744 (2020) <https://doi.org/10.1109/ACCESS.2020.3020917>
- [6] Belazi, A., Talha, M., Kharbech, S., Xiang, W.: Novel medical image encryption scheme based on chaos and DNA encoding. *IEEE Access* **7**, 36667–36681 (2019) <https://doi.org/10.1109/ACCESS.2019.2906292>
- [7] Su, Y., Xia, H., Chen, Z., Chen, H., Huang, L.: A novel one-dimensional chaotic system for image encryption through the three-strand structure of DNA. *Entropy* **27**(8), 776 (2025) <https://doi.org/10.3390/e27080776>
- [8] Xue, X., Zhou, D., Zhou, C.: New insights into the existing image encryption algorithms based on DNA coding. *PLOS ONE* **15**(10), 0241184 (2020) <https://doi.org/10.1371/journal.pone.0241184> . The PLOS ONE Editors issued an Expression of Concern regarding the peer-review process on 7 July 2026, *PLOS ONE* 21(7), e0353144, doi:10.1371/journal.pone.0353144; no author involvement was found
- [9] Wu, Y., Noonan, J.P., Agaian, S.: NPCR and UACI randomness tests for image encryption. *Cyber Journals: Journal of Selected Areas in Telecommunications (JSAT)*, 31–38 (2011)
- [10] Zhang, Q., Guo, L., Wei, X.: Image encryption using DNA addition combining with chaotic maps. *Mathematical and Computer Modelling* **52**(11–12), 2028–2035 (2010) <https://doi.org/10.1016/j.mcm.2010.06.005>
- [11] Hermassi, H., Belazi, A., Rhouma, R., Belghith, S.: Security analysis of an image encryption algorithm based on a DNA addition combining with chaotic maps. *Multimedia Tools and Applications* **72**, 2211–2224 (2014) <https://doi.org/10.1007/s11042-013-1533-6>
- [12] Liu, L., Zhang, Q., Wei, X.: A RGB image encryption algorithm based on DNA encoding and chaos map. *Computers & Electrical Engineering* **38**(5), 1240–1248 (2012) <https://doi.org/10.1016/j.compeleceng.2012.02.007>
- [13] Belazi, A., Hermassi, H., Rhouma, R., Belghith, S.: Algebraic analysis of a RGB image encryption algorithm based on DNA encoding and chaotic map. *Nonlinear Dynamics* **76**, 1989–2004 (2014) <https://doi.org/10.1007/s11071-014-1263-y>
- [14] Chen, J., Chen, L., Zhou, Y.: Cryptanalysis of a DNA-based image encryption scheme. *Information Sciences* **520**, 130–141 (2020) <https://doi.org/10.1016/j.ins.2020.02.024>
- [15] Solak, E.: Cryptanalysis of chaotic ciphers. In: Kocarev, L., Lian, S. (eds.) *Chaos-Based Cryptography. Studies in Computational Intelligence*, vol. 354,

- pp. 227–256. Springer, Berlin, Heidelberg (2011). https://doi.org/10.1007/978-3-642-20542-2_7
- [16] Ping, P., Xu, F., Wang, Z.-J.: Image encryption based on non-affine and balanced cellular automata. *Signal Processing* **105**, 419–429 (2014) <https://doi.org/10.1016/j.sigpro.2014.06.020>
 - [17] Ping, P., Wu, J., Mao, Y., Xu, F., Fan, J.: Design of image cipher using life-like cellular automata and chaotic map. *Signal Processing* **150**, 233–247 (2018) <https://doi.org/10.1016/j.sigpro.2018.04.018>
 - [18] Wang, Y., Cui, W., Tao, Y.: A color image chunking encryption algorithm based on DNA and compound chaotic system. *Multimedia Tools and Applications* **83**, 35449–35469 (2024) <https://doi.org/10.1007/s11042-023-16869-7> . doi:10.1007/s11042-023-16869-7
 - [19] Li, R., Liu, T., Yin, J.: An encryption algorithm for color images based on an improved dual-chaotic system combined with DNA encoding. *Scientific Reports* **14**, 20733 (2024) <https://doi.org/10.1038/s41598-024-71267-9> . doi:10.1038/s41598-024-71267-9
 - [20] Tang, C., Wang, S., Shu, Y., Ren, F.: Encryption algorithm based on improved four-dimensional chaotic system and dynamic DNA encoding. *AIP Advances* **14**, 095226 (2024) <https://doi.org/10.1063/5.0207225> . doi:10.1063/5.0207225
 - [21] Zhang, C., Li, X., Luan, Y., Fan, W.: A chaotic encryption approach improving digital image security. In: *Proc. IEEE Int. Conf. on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, pp. 383–392 (2023). <https://doi.org/10.1109/CyberC58899.2023.00066> . doi:10.1109/CyberC58899.2023.00066
 - [22] Braeken, A., Semaev, I.: The ANF of the composition of addition and multiplication mod 2^n with a Boolean function. In: *Fast Software Encryption (FSE 2005)*. *Lecture Notes in Computer Science*, vol. 3557, pp. 112–125. Berlin, Heidelberg (2005). https://doi.org/10.1007/11502760_8
 - [23] Courtois, N.T., Meier, W.: Algebraic Attacks on Stream Ciphers with Linear Feedback, pp. 345–359. Springer, Berlin, Heidelberg (2003). https://doi.org/10.1007/3-540-39200-9_21
 - [24] Knudsen, L.R.: Truncated and higher order differentials, pp. 196–211. Springer, Berlin, Heidelberg (1995). https://doi.org/10.1007/3-540-60590-8_16
 - [25] Biryukov, A., De Cannière, C., Braeken, A., Preneel, B.: A Toolbox for Cryptanalysis: Linear and Affine Equivalence Algorithms, pp. 33–50. Springer, Berlin, Heidelberg (2003). https://doi.org/10.1007/3-540-39200-9_3

- [26] Mihajloska, H., Gligoroski, D.: Construction of optimal 4-bit s-boxes by quasigroups of order 4. In: SECURWARE 2012: The Sixth International Conference on Emerging Security Information, Systems and Technologies, pp. 163–168. IARIA, Rome, Italy (2012)
- [27] Shcherbacov, V.A.: Quasigroups in cryptology. *Computer Science Journal of Moldova* **17**(2), 193–228 (2009)
- [28] Carlet, C.: *Boolean Functions for Cryptography and Coding Theory*. Cambridge University Press, Cambridge (2021). <https://doi.org/10.1017/9781108606806>
- [29] Nyberg, K.: Differentially uniform mappings for cryptography, vol. 765, pp. 55–64. Springer, Berlin, Heidelberg (1994). https://doi.org/10.1007/3-540-48285-7_6
- [30] Rothaus, O.S.: On “bent” functions. *Journal of Combinatorial Theory, Series A* **20**(3), 300–305 (1976) [https://doi.org/10.1016/0097-3165\(76\)90024-8](https://doi.org/10.1016/0097-3165(76)90024-8)
- [31] Carlet, C., Mesnager, S.: Four decades of research on bent functions. *Designs, Codes and Cryptography* **78**(1), 5–50 (2016) <https://doi.org/10.1007/s10623-015-0145-8>
- [32] Nyberg, K., Knudsen, L.R.: Provable security against a differential attack. *Journal of Cryptology* **8**(1), 27–37 (1995) <https://doi.org/10.1007/bf00204800>
- [33] Leander, G., Poschmann, A.: On the Classification of 4 Bit S-Boxes, vol. 4547, pp. 159–176. Springer, Berlin, Heidelberg (2007). https://doi.org/10.1007/978-3-540-73074-3_13
- [34] Lai, X.: Additive and linear structures of cryptographic functions, pp. 75–85. Springer, Berlin, Heidelberg (1995). https://doi.org/10.1007/3-540-60590-8_6
- [35] Preishuber, M., Hütter, T., Katzenbeisser, S., Uhl, A.: Depreciating motivation and empirical security analysis of chaos-based image and video encryption. *IEEE Transactions on Information Forensics and Security* **13**(9), 2137–2150 (2018) <https://doi.org/10.1109/TIFS.2018.2812080>
- [36] Meier, W., Staffelbach, O.: Analysis of pseudo random sequences generated by cellular automata. In: *Advances in Cryptology — EUROCRYPT ’91. Lecture Notes in Computer Science*, vol. 547, pp. 186–199. Springer, Berlin, Heidelberg (1991)