On the Emergence of Self-Referential Structure in a Torah-Derived RSA System

Principal Investigator & Discoverer: Udi Ben Zvi, Independent Researcher

Academic Advisory and Review Contributions:

Rarity-Evaluation Architecture & Statistical Validation:

Rabbi Oren Evron, Independent Researcher

Correspondence: thesignature.online

1. Introduction

One of the most fundamental problems in human communication is authorship: how can a message prove, beyond assertion, who stands behind it? Modern cryptography was developed to address precisely this problem of trust. Digital signature systems such as RSA provide a mathematically precise mechanism for producing publicly verifiable markers of identity; that is, outputs uniquely determined by their signer.

This study investigates the implications of finding such a signature formalism, instantiated not from engineered cryptographic keys but from numerical values embedded in an ancient sacred text. A twentieth-century mechanism of mathematical authorship, designed for digital communication, is here applied to parameters drawn from a text transmitted for more than three millennia. If the resulting signatures were to exhibit systematic alignment with a claimed author identity—under explicitly defined rules and beyond matched null expectations—one is led to a natural question: how could such convergence arise? Is it merely numerical coincidence, or does it reflect deeper structural organization within the text itself?

RSA (Rivest–Shamir–Adleman), introduced in 1977 and published in 1978, was the first practical and widely deployed public-key cryptosystem that continues to underpin cryptographic infrastructure on the modern internet (Rivest et al., 1978). It is built around modular exponentiation with a semiprime modulus $n = pq$: the public key consists of the pair (n, e), where e is typically chosen as a Fermat prime, while a corresponding private key enables the inverse operation. RSA has two standard uses, encryption and digital signatures, and the present study focuses exclusively on the signature setting.

Unlike encryption, which is used for confidentiality, digital signatures are designed to produce a public and verifiable marker of authorship. The signature framework is therefore the natural RSA setting for an authorship-focused question, and provides a

concrete computational lens through which to examine the possibility of a text-embedded “signature.”

In a digital-signature framework, the private signing key is the identity-bearing component of the system: it is the value used by the signer to generate a publicly verifiable signature. If such a system were instantiated deterministically from text-derived numerical anchors, the analysis to determine this should follow the internal logic of RSA itself. Hence, in this study, the derived private key is first examined as the system’s signer-identity value; second, the signature generated by that key is examined for self-reference to the same identity. In this way, the construction is evaluated at both key level and signature-output level.

The central research question in this study is as follows: *Can a mathematical signature-like structure, instantiated from the text of a book itself, point to the identity behind the book?* In the case of the Torah, this question has occupied historical and theological discourse for millennia. In contrast to previous analysis, this inquiry approaches it through RSA digital-signature formalism, treating text-derived integers as deterministic inputs into a reproducible algebraic system designed precisely to address the source-identity problem already strongly associated with the text.

In this study, we establish the identity alignment at key level (Section 3), and then examine the corresponding signature behavior. In a digital-signature framework, the natural message to sign when testing authorship is the author's name itself. Accordingly, we encode *Havaya* using its regular gematria and compute its RSA signature using the derived private signing key, revealing that the resulting output relates back to the signed author value under the algebraic rules of conventional RSA.

However, a single construction—even one arising from unusually clean numerical parameters—cannot by itself distinguish structural organization from coincidence. Although this carefully chosen anchor has produced a suggestive alignment, the essential question is whether such alignments arise more frequently than would be

expected when the same construction rules are applied uniformly across the Torah's vocabulary.

For this reason, this study evaluates the *Torah* construction within a broader randomized framework (Sections 4 and 5). Rather than privileging specific canonical locations in the text, we treat the Torah words themselves as potential RSA anchors. Words are sampled uniformly from the Torah's distinct vocabulary and tested for RSA admissibility under the same numerical conventions. Only those whose regular gematria forms a semiprime modulus and whose small gematria yields a valid Fermat-prime exponent are retained.

For each RSA-valid instance, multiple candidate author names are sampled from the same vocabulary, and the instance is retained only if the RSA-derived private key coincides with one of them; only then is the signature computed and tested under the pre-declared pattern catalog.

In this way, the Torah case anchored in the word *Torah* is no longer examined in isolation. Instead, it becomes one instance within a large generative experiment governed by the same algebraic constraints. The question then shifts from anecdotal alignment to statistical analysis, and the results prove that the Torah reference outcome arise with unusual rarity when compared with uniformly generated corpus-based controls.

1.1 Background and Motivation

The regular gematria of the Torah's opening verse, "בראשית ברא אלהים את השמים ואת הארץ," is 2,701, and this value is the following semiprime:

$$2701 = 37 \times 73.$$

From a cryptographic perspective, this fact is immediately suggestive. Since a semiprime modulus is the core structural requirement of RSA, it is natural to ask whether the opening verse could be used to construct an RSA-like system and whether

such a construction would produce meaningful or structured behavior. The construction of an initial RSA system from numerical values associated with the opening verse produced a group of nontrivial numerical patterns, prompting the need for a more careful evaluation of rarity and statistical significance in a broader numerical context.

In previous work, Rabbi Oren Evron investigated Genesis 1:1 to determine whether the Torah's opening description of creation exhibits a structured numerical correspondence with π, one of the most fundamental mathematical constants associated with physical and geometric reality. Because Genesis 1:1 describes the creation of the heavens and the earth, it served as the natural textual anchor for that inquiry. Evron found that the sum of the first 611 digits of π equals 2,701, linking 611—the regular gematria of *Torah*—with 2,701, the regular gematria of Genesis 1:1. Moreover, the sum of the first 17 digits of π equals 82, linking 17—the small gematria of *Torah*—with 82, the small gematria of Genesis 1:1 (Evron, *Pi & Genesis*, 2026).

Evron's contributions in the present study led to a refinement of its textual anchor. While Genesis 1:1 was the natural anchor for Evron's creation-focused π inquiry, the present study asks a different question that is related to authorship. For this reason, the present RSA construction is anchored in the most fundamental textual marker of the work itself: its name, *Torah*.

2. Preliminaries

2.1 Gematria Conventions and Transforms

Throughout this paper, Hebrew text is mapped to integers using fixed gematria conventions. These rules, defined here, are applied uniformly in all subsequent constructions.

2.1.1 Regular Gematria (*mispar hechrechi*)

We use the standard gematria system in which Hebrew letters are assigned values from 1 to 400:

א=1, ב=2, ג=3, ד=4, ה=5, ו=6, ז=7, ח=8, ט=9, י=10, כ=20, ל=30, מ=40, נ=50, ס=60, ע=70, פ=80,
צ=90, ק=100, ר=200, ש=300, ת=400

Final letter forms are assigned the same values as their non-final counterparts. The regular gematria of a word or phrase is the sum of its letter values.

2.1.2 Small Gematria (*mispar katan*)

Small gematria is defined by removing the trailing zeros from each letter's regular gematria value:

א=1, ב=2, ג=3, ד=4, ה=5, ו=6, ז=7, ח=8, ט=9, י=1, כ=2, ל=3, מ=4, נ=5, ס=6, ע=7, פ=8, צ=9, ק=1,
ר=2, ש=3, ת=4

2.2 RSA Signatures: Parameters and Notation

2.2.1 Key Generation and Parameters

An RSA signature system begins by choosing two distinct odd primes p and q and forming the modulus

$$n = pq.$$

Let φ(n) denote Euler's totient function. For *n=pq*,

$$\varphi(n) = (p - 1)(q - 1).$$

The public key value *e* is chosen such that

$$1 < e < \varphi(n) \; and \; gcd(e, \varphi(n)) = 1.$$

In other words, *e* is coprime with *φ*(*n*). The private key *d* is defined as the modular inverse of $e\ modulo\ \varphi(n)$:

$$ed \equiv 1 (mod \varphi(n)).$$

In practical implementations, the public key value *e* is chosen from the Fermat primes because these values make verification especially efficient. The known Fermat primes are 3, 5, 17, 257, and 65,537, with 65,537 widely used as the modern default (and smaller values such as 3 and 17 appearing historically).

2.2.2 Signature and Verification

RSA signatures operate on an integer message value *m*. The signer uses the private signing key *d* to compute the signature

$$s = m^d mod n.$$

The pair (*m*, *s*) may then be transmitted. Verification is performed using the public exponent *e*. The verifier computes

$$v = s^e mod n$$

and compares *v* with the claimed message value *m*. If *v* = *m*, the signature is accepted as valid. In other words, the public-key check succeeds, and the message is treated as originating from the holder of the private signing key.

3. The Case of The Torah

Because the topic of this study concerns the identity behind the book as a whole, the natural starting point is the most fundamental textual anchor associated with the work itself: its name, “תורה” (*Torah*). In the case of *Torah*, the alignment is especially clean. The regular gematria of *Torah* is 611, and

$$611 = 13 \times 47,$$

which is a semiprime modulus of the RSA form *n=pq*. Moreover, its small gematria is 17, which is a Fermat prime. Together, these values supply exactly the two public parameters required to instantiate an RSA system defined as *(n,e)=(611,17)*.

Because the construction is designed to examine authorship, the expected author-linked values are specified in advance. Within Jewish tradition, the Torah is explicitly attributed to יהו״ה (*Havaya*) and is therefore commonly referred to as "תורת יהו״ה" (*the Torah of Havaya*). Accordingly, if a signature-like structure were present, the natural expectation would be to encounter the Divine name itself. The regular and small gematria of *Havaya* are 26 and 17, respectively. However**,** in classical Torah literature, *Havaya* is canonically paired with אדנ"י (*Adonai*) as two aspects of a single Divine identity. This relationship is especially evident in traditional practice, where *Havaya* remains the written name, while *Adonai* serves as its spoken form. The regular and small gematria of *Adonai* are 65 and 11, respectively. Consequently, within the specified context of this investigation, the appearance of either 26 (*Havaya*) or 65 (*Adonai*) are candidate author-linked values. To allow additional degrees of freedom in a conservative manner, further Divine names that might reasonably be associated with authorship—such as אלהי"ם (*Elohim*), שד"י (*Shadai*), and א"ל (*El*) —are also included among the candidate identities.

Under this framework, the RSA system defined by (611, 17) determines a private signing key whose numerical value is 65. This value corresponds exactly to the regular gematria of *Adonai*. The derived private key therefore yields not an arbitrary number but a value directly associated with the claimed authorial identity of the book.

As noted above, although this case leads to a highly unexpected result, its significance must be considered in a larger context. Hence, the next section describes the experiments used in the statistical analysis to determine if the Torah reference outcome arises with unusual rarity when compared with uniformly generated corpus-based controls.

4. Methodology

4.1 Experimental Pipeline Overview

This section describes the randomized signing-and-scoring pipeline used throughout the study. Each run—whether the Torah reference case or a Monte Carlo control trial—follows the same deterministic procedure; only the sampled Torah vocabulary items differ.

Each trial begins by selecting a single Torah word and treating it as a candidate "book name." The restriction to a single-token book name is intentionally conservative (see Appendix F for its empirical justification). From this word, the RSA public parameters are derived directly using its regular and small gematria. The regular gematria supplies the modulus candidate and must factor as a semiprime $n = pq$ with distinct odd primes. The small gematria supplies the public exponent and must be one of the standard Fermat-prime values used in RSA. The assignment of gematria types to RSA parameters is not interchangeable: reversing the mapping (that is, using the regular gematria for the exponent and the small gematria for the modulus) produces no RSA-valid instances in the Torah vocabulary and therefore introduces no additional degree of freedom in the pipeline.

A book-name word is considered RSA-valid when this modulus–exponent pair satisfies the standard structural requirements of RSA and uniquely determines a private signing key (see Appendix A for the formal RSA validity conditions). Trials that do not yield a valid RSA system cannot produce a private signing key; consequently, the pipeline cannot continue beyond this point, and these trials are recorded as no-match instances.

For the RSA-valid instances, a symmetry-controlled author selection stage is applied. Five distinct Torah words are sampled uniformly from the same vocabulary and designated as candidate author names—one primary and four secondary. The RSA-derived private signing key must coincide with the regular gematria of at least one

of these five names, implementing the identity-alignment condition; otherwise, the trial is discarded (see Appendix A for a formal trial construction).

The observed reference alignment occurs with *Adonai*, the most a priori secondary identity traditionally paired with *Havaya*. Methodologically, the construction could therefore have been restricted to a primary author name and a single secondary candidate. Instead, the pipeline allows five candidate names, introducing additional degrees of freedom. These additional candidates are not required for the reference case; by contrast, they expand the opportunity space available to the control trials, making the null model more permissive and the overall analysis more conservative.

For the surviving trials, the RSA signature of the primary author name is computed and evaluated under a fully pre-declared catalog of algebraic match rules (see Appendix B). These rules test for structured self-reference between the signature output and the gematria values of each candidate author identity in the set (primary and secondary). Each satisfied rule produces a labeled outcome; the set of all recorded labels constitutes the trial's pattern set.

In the Torah reference case, exactly one rule is satisfied, and hence the reference pattern set contains a single recorded outcome. Rarity is assessed by comparing this reference pattern set to those generated under large-scale Monte Carlo trials executed under an identical pipeline.

A naïve Monte Carlo approach might score trials by simply counting how many rules are satisfied, or by assigning weights to different rule families. We do not adopt such scoring. Many rule outcomes are algebraically related and are therefore not statistically independent; simple match-counting risks overstating the evidence by implicitly treating dependent structures as separate signals. Moreover, weighted scoring introduces subjective choices that are difficult to justify.

Instead, rarity is evaluated using a subset-support statistic. This method treats the reference pattern set as a structured object and asks how often the null model

produces pattern sets that contain it. By evaluating containment rather than raw counts, the procedure avoids implicit independence assumptions and removes the need for arbitrary weighting. The formal definition of the subset-support score and Monte Carlo p-value is given in Appendix C.

4.2 Reference Case Within the Pipeline

The Torah reference case is evaluated under the identical RSA construction described above. The book name *Torah* yields the RSA system (*n*, *e*) = (611, 17), which satisfies the RSA-validity conditions.

For the reference instantiation, the candidate author set consists of the principal Divine names that are traditionally associated with the identity of the author of the Torah: *Havaya, Adonai, Elohim, Shadai, El*.

As defined in the pipeline, the instance proceeds only if the RSA-derived private signing key matches the regular gematria of at least one name in this author set.

For the system (611,17), the RSA private signing key is

$$d=65.$$

Since 65 is the regular gematria of *Adonai*, the reference case satisfies the author–key alignment requirement and the analysis proceeds to signature computation.

The RSA signature of the designated primary author name *Havaya* (regular gematria 26) is then computed and evaluated under the same pre-declared catalog of algebraic match rules used in all Monte Carlo trials.

5. Results

5.1 Signature Outcome for the Torah Reference Case

Under the RSA system (*n, e*) = (611, 17), the private signing key is (*d* = 65). The designated primary author name is *Havaya*, whose regular gematria value is

$$m = 26.$$

The RSA signature is computed as

$$signature(26) = 26^{65} \, mod \, 611 = 442$$

since

$$442 = 26 \times 17.$$

The signature exhibits a self-referential structure: it combines 26, the regular gematria value of the Divine name *Havaya*, with 17, its small gematria value, thereby representing the name multiplied by itself across two of its most standard gematria encodings.

No further matches are observed. In other words, the signature value 442 corresponds only to the primary author and not to the four secondary names—*Adonai*, *Elohim*, *Shadai,* or *El*.

The Torah reference pattern set therefore contains a single recorded outcome.

5.2 Monte Carlo Significance

To assess rarity under the identical pipeline, we generated *N*=100,000,000,000 Monte Carlo trials (100 billion). The reference subset-support score was

$$R_{ref} = 5{,}843.$$

Across all trials, 24,693 control trials exhibited subset-support scores less than or equal to R_{ref}. The resulting Monte Carlo p-value is therefore

$$P = 2.46 \times 10^{-7},$$

corresponding to approximately one occurrence in 4,049,730 trials under the null model (Robert & Casella, 2004). The observed outcome lies several orders of magnitude below conventional thresholds for statistical rarity.

5.3 Exploratory Deterministic Extensions

Although the statistical analysis above is restricted to the randomized book-name pipeline, the same RSA framework can be extended deterministically to additional canonical textual anchors. In practical digital-signature systems, the public exponent is typically fixed, while distinct signature systems are generated by varying the modulus. We mimic this structure here; the exponent *e* = 17, derived from the most a priori textual anchor (the book name) is held fixed, and additional signing systems are generated by substituting moduli derived from the next most a priori elements of any book, namely the opening word and the opening verse. Under this fixed-exponent framework, further structured correspondences emerge.

5.3.1 Deterministic Anchor Variants

In addition to the base anchor values derived from regular gematria, we consider a small set of simple deterministic variants. These include the Sum-of-Thousands (SoT) reduction, an enlarged-letter gematria convention, and a center-point transform. The SoT and center-point transforms appear in Evron's earlier analyses of the Torah's opening verse, where they participate in several structured relationships derived from the opening text (Evron, *Genesis 1:1 research materials*, 2026).

For example, 2,701 → 2 + 701 = 703 under the SoT reduction, an operation referred to in the kabbalistic literature as חזרה חלילה, and the center point of 2,701 is 1,351.

The enlarged-letter variant reflects a traditional scribal feature of the Torah text, in which certain letters appear in enlarged form. In the Torah's opening word, the initial letter ב (*Beit*) is enlarged—the only enlarged *Beit* in the Torah. Under this convention, the letter contributes 2,000 rather than its regular value of 2, thereby increasing the opening-verse gematria value from 2,701 to 4,699.

5.3.2 The Opening Word בראשית (*Bereshit*)

The opening word "בראשית" has a regular gematria of 913, with factorization

$$913 = 11 \times 83.$$

Using $e = 17$, the resulting RSA system is

$$n = 913,\ e = 17,\ d = 193.$$

Signing the author value gives

$$signature(26) = 26^{193} mod 913 = 702.$$

Since

$$702 = 26 \times 27,$$

the signature again shows a self-referential form, as the output factors through the author value (26).

5.3.3 The Opening Verse בראשית ברא אלהים את השמים ואת הארץ (*Bereshit bara Elohim et hashamayim ve'et haaretz*)

The first verse, "בראשית ברא אלהים את השמים ואת הארץ" has a regular gematria of 2,701, and

$$2{,}701 = 37 \times 73.$$

Using $e = 17$, the resulting RSA system is

n = 2,701, e = 17, d = 305.

Signing the author value gives

$$signature(26) = 26^{305} mod 2701 = 232.$$

The value 232 (רל״ב) equals the sum of the four traditional spellings of *Havaya*

ע״ב + ס״ג + מ״ה + ב״ן,

as described in classical kabbalistic literature. In this case, the signature again exhibits self-reference to *Havaya* through one of the most established kabbalistic structures built around the Divine name: its four principal written expansions, which together sum to 232.

5.3.4 The Opening Verse — SoT

Applying the SoT to 2,701 yields 703, and

$$703 = 19 \times 37.$$

Using *e* = 17, the resulting RSA system is

n = 703, e = 17, d = 305.

Signing the author value gives

$$signature(26) = 26^{305} mod 703 = 676\,.$$

Since

$$676 = 26^2,$$

the self-reference here is especially strong: the signature lands exactly on the author value squared.

5.3.5 The Opening Verse — The Enlarged Beit

Under the enlarged-letter convention, the opening-verse value becomes 4,699, and

$$4{,}699 = 37 \times 127.$$

Using *e* = 17, the resulting RSA system is

$$n = 4{,}699,\ e = 17,\ d = 1{,}601.$$

Signing the author value gives

$$signature(26) = 26^{1601} mod 4699 = 1{,}231.$$

The value 1,231 equals the regular gematria of the traditional kabbalistic written-form of the number 26, "עשרים ושש" ("twenty-six"), as noted by the 13th-century kabbalist Rabbi Joseph ben Abraham Gikatilla (*Ginat Egoz*). In this case, the signature returns to the author value through its written Hebrew expression.

5.3.6 The Opening Verse — The Center Point

Applying the center-point transform to 2,701 gives

$$1{,}351 = 7 \times 193.$$

Using *e* = 17, the resulting RSA system is

$$n = 1{,}351,\ e = 17,\ d = 881.$$

Signing the author value obtains

$$signature(26) = 26^{881} mod 1351 = 1{,}081.$$

The value 1,081 is the gematria of the sefira תפארת (*Tiferet*). In kabbalistic tradition, the sefirot are the principal modes through which Divine emanation is described, and תפארת

is specifically associated with *Havaya*. The signature therefore returns to the exact sefira traditionally paired with the Divine name being signed.

5.3.7 Statistical Scope and Structural Recurrence

These deterministic extensions are not included in the Monte Carlo subset-support analysis reported above, and therefore do not contribute to the computed p-value. They are presented as structural continuations of the same fixed-exponent RSA framework. While the statistical test is anchored strictly in the randomized book-name pipeline, the recurrence of author-linked structure across independently derived moduli from the opening word and opening verse strengthens the coherence of the overall construction. The observed pattern is therefore not confined to a single anchor but reappears across the text's most a priori structural elements.

6. Discussion

This study examined whether an RSA signature systems instantiated from Torah book-name candidates—words sampled uniformly from the Torah's distinct vocabulary and mapped to RSA parameters via gematria—exhibit author-linked structure beyond what would be expected under matched randomization of the same corpus.

The Torah reference case is obtained by taking the book name *Torah*, which defines the RSA system (n, e) = (611, 17). Within the pipeline, this construction satisfies a two-level identity-consistency question natural to digital signatures: whether the derived private signing key aligns with a candidate author identity, and whether the resulting signature output exhibits algebraic self-reference to that same identity under pre-declared rules. In the Torah reference instantiation, the derived signing key is d = 65 (*Adonai*), and signing m = 26 (*Havaya*) yields a signature value that factors into *Havaya*'s two most standard gematria values: 26, its regular value, and 17, its small value.

To evaluate whether such an outcome could plausibly arise under corpus-matched randomness, we implemented a large-scale Monte Carlo null process that applied the identical pipeline to uniformly sampled Torah vocabulary items. Under this null model, the observed reference pattern set occurs with an estimated probability of

$$P = 2.46 \times 10^{-7},$$

corresponding to approximately one occurrence in 4,049,730 trials.

The statistical inference rests on the randomized book-name pipeline and subset-support significance test. Within that defined framework, the Torah reference outcome is highly unlikely to arise under corpus-level random variation.

The further deterministic extensions to the opening word and opening verse, although not included in the Monte Carlo p-value computation nonetheless reinforce the structural coherence of the framework by demonstrating recurrence across independently derived moduli under a fixed exponent, mirroring the architecture of practical digital-signature systems.

This most striking aspect of this phenomenon is the timeline over which it has occurred: a twentieth-century public-key signature formalism, instantiated from Torah-derived numerical encodings under pre-declared rules, yields outputs that repeatedly point back to candidate author identities. This occurs even though the framework was specified in advance and applied uniformly across randomized controls. If the defined null model fails to account for the observed structure, then the most parsimonious interpretation is that the organization is not incidental but intentional—that the text exhibits deliberate self-referential numerical architecture, detectable through mathematical tools developed millennia later.

The findings of this study are grounded in numerical analysis and the field of cryptography, and broader theological interpretation is therefore outside its scope.

However, these findings may have significant implications from a theological perspective that remain to be explored in future work.

References

Evron, O. (2026). *Genesis 1:1 research materials*. The First Verse. https://www.thefirstverse.com

Evron, O. (2026). *Pi & Genesis: Initial study*. The First Verse. https://www.thefirstverse.com/en/research/Pi-Genesis-Initial-Study

Gikatilla, J. ben A. *Ginat Egoz*. Hanau. https://hebrewbooks.org/9423

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

Robert, C. P., & Casella, G. (2004). *Monte Carlo statistical methods* (2nd ed.). Springer.

Appendix A. Trial Construction and RSA Validity

This appendix provides the formal specification of a single trial in the randomized signing-and-scoring pipeline.

A.1 Book-Name Selection

A single word is sampled uniformly from the set of distinct word-types appearing in the Torah corpus. This word is designated as the candidate “book name” for the trial. No weighting by frequency is applied at this stage; sampling is uniform over unique vocabulary items.

A.2 RSA Parameter Derivation and Validity

For a sampled book-name word, we define the following:

- n: its regular gematria value (the candidate modulus),
- e: its small gematria value (the candidate public exponent).

The candidate word is considered RSA-valid only if all of the following conditions hold:

1) Semiprime Modulus:

The regular gematria value must factor as

$$n = pq,$$

where p and q are two distinct ($p \neq q$) odd primes.

2) Fermat-Prime Exponent Constraint:

The small gematria value must satisfy

$$e \in \{3,5,17,257\}.$$

3) RSA Invertibility Condition:

Let $\varphi(n)$ denote Euler's totient function. For $n = pq$,

$$\varphi(n) = (p - 1)(q - 1),$$

the exponent must satisfy

$$1 < e < \varphi(n) \text{ and } \gcd(e, \varphi(n)) = 1.$$

4) Private Signing Key Existence:

When the above conditions hold, the private signing key d is defined as the modular inverse of e modulo $\varphi(n)$ as

$$ed \equiv 1 (\mathrm{mod} \varphi(n)).$$

If any of the above conditions fail, the candidate book name is not RSA-valid. The trial is recorded as a no-match instance and does not proceed to author selection or signature testing.

A.3 Author Selection and Identity Alignment

For RSA-valid instances, five distinct words (one primary author and four secondary authors) are sampled uniformly without replacement from the same Torah vocabulary and designated as candidate author names. The trial proceeds only if the RSA-derived private signing key d equals the regular gematria of at least one of these five candidate author names. If no such equality occurs, the trial is discarded and recorded as a no-match instance. This identity-alignment requirement implements the author-consistency condition described in the main text.

Appendix B. Signature Match Rules and Recording Conventions

This appendix defines the pre-declared algebraic rule families used to evaluate the RSA signature outputs.

Let

- *m* = regular gematria of the primary author;
- *s* = the RSA signature value of *m*;
- For each candidate author a,
  - a_{reg} = the regular gematria value of a;
  - a_{small} = the small gematria value of a.

Each rule is tested against all five candidate author names (one primary and four secondary).

B.1 Rule 1 — Regular Gematria Exact Power

The signature satisfies Rule 1 if

$$s = a_{reg}^{\,i}, \text{ for some } i \geq 1.$$

Label format:

REGULAR_EXACT_POWER_I{i}_COUNT{c}

Here, *c* is the number of authors (out of five) satisfying the same exponent *i*.

B.2 Rule 2 — Regular × Small Exact Powers

The signature satisfies Rule 2 if

$$s = a_{regular}{}^{i} \times a_{small}{}^{j}$$, where $i, j \geq 1$.

Label format:

REGULAR_MULT_SMALL_EXACT_POWERS_I{i}_J{j}_COUNT{c}

If multiple decompositions exist, the maximum regular exponent *i* is recorded.

B.3 Rule 3 — Regular Power with Arbitrary Multiplier

The signature satisfies Rule 3 if

$$s = k \times a_{regular}{}^{i}$$, where $i \geq 1$, $k > 1$.

Label format:

REGULAR_POWER_ARBITRARY_MULT_I{i}_COUNT{c}

The multiplier *k* is not recorded.

Rule 3 is evaluated only if Rule 2 does not match, since Rule 2 is algebraically contained within Rule 3. If multiple exponents are possible, the maximum *i* is recorded.

B.4 Rule 4 — Small Gematria Exact Match

The signature satisfies Rule 4 if

$$s = a_{small}.$$

Label format:

SMALL_EXACT_VALUE_COUNT{c}

B.5 Rule 5 — (Regular + Small) Exact Power

The signature satisfies Rule 5 if

$$signature = (a_{regular} + a_{small})^{i}, i \geq 1.$$

Label format:

REGULAR_PLUS_SMALL_EXACT_POWER_I{i}_COUNT{c}

B.6 Rule 6 — (Regular + Small) Power with Arbitrary Multiplier

The signature satisfies Rule 6 if

$$s = k * (a_{regular} + a_{small})^{i}, i \geq 1, k > 1.$$

Label format:

REGULAR_PLUS_SMALL_POWER_ARBITRARY_MULT_I{i}_COUNT{c}

The multiplier *k* is not recorded. If multiple exponents are possible, the maximum *i* is recorded.

B.7 Recording Policy and Overlaps

All the rule families defined above were evaluated for each of the five candidate authors in a trial.

Rule 3 (regular power with arbitrary multiplier) was evaluated only if Rule 2 (regular × small exact powers) did not match, since Rule 2 is algebraically contained within Rule 3 and would otherwise produce systematic double counting.

No other gating conditions were applied. If a signature satisfied multiple distinct rule families, all applicable matches were recorded. Such overlaps arise only from specific numerical relationships between an author's regular and small gematria values and were treated as meaningful structural outcomes rather than filtered artifacts.

For each rule label, the COUNT{c} component recorded the number of candidate authors (out of five) satisfying the same rule structure within the trial. Higher values of *c* therefore indicate stronger multi-author agreement under that rule.

The set of all recorded labels constitutes the trial's final pattern set.

Appendix C. Subset-Support Statistics and Monte Carlo p-values

This appendix defines the statistical procedure used to evaluate the rarity of the Torah reference outcome under the null model.

C.1 Trial Output Representation

Each trial that survived RSA-validity and identity-alignment produced a pattern set, defined as the set of all rule labels triggered by the signature evaluation stage. Trials that failed RSA validity or identity alignment produced an empty pattern set.

C.2 Subset-Support Definition

Let P_i denote the pattern set of trial *i,* and P_{ref} denote the pattern set of the Torah reference case. A control trial *i* is said to *support* the reference outcome if

$$P_{ref} \subseteq P_i .$$

That is, every label appearing in the reference pattern set must also appear in the control trial's pattern set. The control may contain additional labels.

C.3 Reference Subset-Support Score

The reference subset-support score is defined as

$$R_{ref} = \#\{ i : P_{ref} \subseteq P_i \},$$

which is the number of Monte Carlo trials whose pattern sets contain the full reference pattern set. Smaller values of R_{ref} indicate greater rarity under the null condition.

C.4 Symmetric Trial Scoring

For symmetry, each Monte Carlo trial i was assigned its own subset-support score as follows:

$$R_i = \#\{j : P_i \subseteq P_j\}.$$

This ensured that the reference outcome was evaluated under the same containment rule applied to all trials.

C.5 Monte Carlo p-Value

Let N denote the total number of Monte Carlo trials. The Monte Carlo p-value is defined as

$$p = \#\{i : R_i \leq R_{ref}\}/N.$$

This definition measures how often a randomly generated trial yields a subset-support score at least as rare as the reference outcome under the same containment criterion.

Appendix D. Text Preprocessing and Anchor Extraction

All computations in this study were performed on canonical unvocalized Hebrew text. Niqqud and punctuation marks were removed prior to gematria evaluation. Final letter forms were assigned the same values as their non-final counterparts, consistent with the conventions stated in Section 2.1.

Anchor extraction was deterministic: the “opening word” was defined as the first token of the book’s canonical opening verse under the traditional split, and the “opening verse” was defined as the full first verse under standard segmentation.

Appendix E. Implementation Notes

The Monte Carlo simulations were implemented in Python 3.9. Large-scale simulations were executed in parallel for computational efficiency. Each worker process initialized its pseudorandom number generator with an independent seed to avoid overlapping random streams. Parallelization affected runtime only and did not alter the definition of the null model nor the statistical procedure.

Appendix F. Conservativeness of the Single-Token Book-Name Design

The Monte Carlo pipeline restricts candidate book names to a single Torah word. This design choice is intentionally conservative.

To quantify how the number of tokens in a candidate title affects the likelihood of producing an RSA-valid parameter pair, we conducted an auxiliary experiment in which candidate titles were constructed by randomly sampling words from the Torah's distinct vocabulary and concatenating them into titles of fixed length. For each title length, 100M random samples were generated and evaluated under the same gematria conventions and RSA-validity conditions used in the main pipeline.

The observed approximate probabilities of generating an RSA-valid system are shown in Table F1.

Table F1. Observed approximate probabilities of generating an RSA-valid system for various numbers of tokens in the candidate title.

Number of tokens in the candidate title	Approximate probability of an RSA-valid system
1	~1 in 84
2	~1 in 2,537
3	~1 in 1,149,425

These results show that the probability of producing RSA-valid parameters decreases sharply as the number of tokens increases. Restricting the null model to single-token titles therefore raises the baseline rate of RSA-valid constructions, making successful matches easier to obtain under the null model and thus rendering the statistical test more conservative.

To compare this restriction with a real-world title structure, we analyzed Hebrew book titles from the online catalogs of the Israeli retailers צומת ספרים (Booknet) and סטימצקי (Steimatzky). Titles were collected through automated catalog extraction, supplemented by approximately 150 additional titles aggregated with the assistance of Gemini 3 to broaden catalog coverage.

Titles containing non-Hebrew characters were excluded. Entire titles were also filtered out if they contained tokens associated with edition metadata, volume indicators, publishing information, format descriptors, educational materials, or marketing labels (e.g., “מבצע”, “תרגול”, “קומיקס”, “תרגום”, “כרך”, “מהדורה”). Titles longer than six tokens were excluded, and duplicate titles were removed. After applying these filters, the dataset contained 14,342 unique titles. The distribution of title lengths is shown in Table F2.

Table F2. Distribution of Hebrew book title lengths

Number of Tokens	Count	Percentage
1	1,808	12.61%
2	5,793	40.39%
3	3,923	27.35%

4	1,819	12.68%
5	726	5.06%
6	273	1.90%

In this dataset, 87.39% of titles contain two or more tokens, whereas only 12.61% consist of a single token. Consequently, the experimental design used in this study, which restricted candidate book names to a single token, allowed RSA-valid anchors to arise far more frequently than would occur under typical multi-token title formation. The null model therefore provides a relatively permissive baseline, reinforcing the conservative character of the statistical test.