International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2025: 7.089

A Reliability-Theoretic Framework for Deterministic RSA Exponent Generation Using Linear Diophantine Equations

Dr. C. Manjula[1], Dr. Chaya Kumari Divakarla[2]

[1]Associate Professor & HoD, Department of Mathematics, AMC Engineering College, Bangalore-560083, India
Email: *manjula.prathap[at]amceducation.in*

[2]Associate Professor, Department of Mathematics, AMC Engineering College, Bangalore-560083, India
Email: *chayakumari.divakarla[at]gmail.com*

Abstract: ***The deterministic generation of cryptographic parameters has become increasingly important in applications requiring transparency, reproducibility, and formal verification. This paper introduces a reliability-theoretic framework for deriving the public exponent of an RSA cryptosystem from the structured mathematical model. In the proposed methodology, the public encryption exponent is deterministically derived from the reliability polynomial associated with a documented network topology. Subsequently, the corresponding private decryption exponent is computed by solving the linear Diophantine equation$ed \equiv 1 \pmod{\varphi(n)}$ using the Extended Euclidean Algorithm. This procedure preserves the algebraic framework of the classical RSA cryptosystem while introducing a mathematically reproducible mechanism for public exponent generation. To demonstrate the proposed methodology, a five-component Wheatstone bridge network is employed as the underlying reliability model. The reliability polynomial of the network is first constructed and subsequently used to generate the public exponent. The remaining stages of RSA key generation, encryption, and decryption follow the standard cryptographic procedures. The mathematical correctness of the proposed framework is established through theoretical analysis, and its computational characteristics are compared with those of the conventional RSA algorithm. The results indicate that the proposed approach retains the computational efficiency and security properties of classical RSA while providing a deterministic, traceable, and verifiable key-generation methodology. Such a framework is particularly well suited to engineering applications in which documented reliability models and cryptographic infrastructures coexist, thereby facilitating greater accountability, reproducibility, and trust in cryptographic key management.***

Keywords: Public-key cryptography; Reliability polynomial; Coherent systems; Linear Diophantine equations; RSA cryptosystem; Extended Euclidean Algorithm; Structure function; Number theory; Mathematical cryptography

1. Introduction

The rapid expansion of secure digital communication has intensified the demand for cryptographic techniques that combine strong mathematical foundations with reproducible parameter generation. Public-key cryptography constitutes one of the most influential developments in modern information security, enabling confidential communication, authentication, and digital signatures over insecure networks. Since the pioneering work of Diffie and Hellman introduced the concept of public-key exchange, numerous cryptographic systems have been proposed based on computationally difficult mathematical problems, among which the RSA cryptosystem remains one of the most widely deployed.

The security of RSA depends fundamentally upon the computational intractability of factoring the product of two large prime integers. Although the theoretical foundations and practical implementation of RSA have been extensively investigated, comparatively little attention has been devoted to the mathematical origin of the public encryption exponent. In conventional implementations, the exponent is selected from a set of integers satisfying the coprimality condition with Euler's totient function. Frequently, a fixed value such as 65537 is employed because of its computational efficiency. While such choices are mathematically valid, they possess limited structural significance and provide no intrinsic mechanism for documenting the provenance of the selected parameter.

Reliability theory offers a complementary mathematical discipline concerned with the analysis of engineering systems composed of interconnected components. A coherent system is represented by a structure function that characterizes the operational state of the entire system in terms of the states of its individual components. The combinatorial properties of minimal path sets and minimal cut sets enable the construction of a reliability polynomial, which completely describes the probability of successful system operation under assumptions of component independence. Because the coefficients of this polynomial depend solely on the underlying system topology, they constitute deterministic combinatorial invariants.

The present work establishes a connection between these two seemingly unrelated mathematical disciplines. Instead of selecting the RSA public exponent through an arbitrary procedure, the exponent is generated deterministically from the integer evaluation of a reliability polynomial associated with a coherent engineering network. The corresponding private exponent is then computed as the unique modular inverse obtained by solving a linear Diophantine equation using Bézout's identity and the Extended Euclidean Algorithm.

Unlike alternative public-key systems that introduce entirely new computational assumptions, the proposed construction deliberately preserves the classical RSA security model. The reliability polynomial serves only as a mathematically reproducible source of public parameters and does not replace the integer factorization problem. Consequently, the proposed framework inherits the well-established theoretical properties of RSA while introducing an auditable mechanism that links cryptographic parameters to formally documented engineering structures.

Beyond its practical motivation, the proposed methodology illustrates an interdisciplinary interaction between reliability theory, combinatorial mathematics, number theory, and public-key cryptography. Such integration broadens the mathematical interpretation of cryptographic parameter generation and demonstrates how combinatorial invariants derived from engineering systems may contribute to reproducible cryptographic design without altering the underlying security assumptions.

Conventional RSA implementations generate the public exponent from a comparatively small set of admissible integers satisfying elementary number-theoretic conditions. Although computationally efficient, this process provides no systematic explanation for why a particular exponent was selected. In environments involving safety-critical infrastructure, industrial automation, or engineering systems subject to formal auditing, reproducibility and traceability of cryptographic parameters are desirable complementary properties.

Reliability engineering naturally produces deterministic mathematical objects through the analysis of coherent systems. Since the reliability polynomial uniquely reflects the topology of the underlying network, it offers an attractive mathematical source for generating reproducible cryptographic parameters. This observation motivates the present study.

The main contributions of this work are summarized as follows.

1) A deterministic framework for generating RSA public exponents from reliability polynomials of coherent systems.
2) A mathematical integration of reliability theory and public-key cryptography without modifying the classical RSA algorithm.
3) An explicit formulation of RSA key generation as the solution of a linear Diophantine equation.
4) A reproducible and auditable methodology for parameter generation based on combinatorial invariants.
5) A complete numerical example demonstrating key generation, encryption, and decryption.
6) A theoretical discussion comparing the proposed framework with conventional RSA and existing Diophantine-based cryptographic constructions.

2. Organization of the Paper

The Paper is organized as follows. Section 2 reviews the mathematical concepts from reliability theory, coherent systems, and linear Diophantine equations required for the proposed construction. Section 3 surveys existing research related to RSA, reliability polynomials, and Diophantine cryptography. Section 4 presents the proposed deterministic exponent-generation algorithm. Section 5 develops the mathematical analysis and correctness results. Section 6 provides computational examples and complexity analysis. Section 7 discusses the security properties and compares the proposed framework with existing public-key schemes. Finally, Section 8 summarizes the principal conclusions and outlines potential directions for future research.

Mathematical Preliminaries

This section presents the mathematical foundations underlying the proposed reliability-theoretic RSA framework. The discussion integrates concepts from reliability theory, graph theory, number theory, and public-key cryptography employed in the proposed cryptosystem.

2.1 Coherent Systems and Structure Functions

Let $X=(x_1,x_2,...,x_n)$, where $x_i \in \{0,1\}$. Here $x_i=1$ denotes a functioning component and $x_i=0$ denotes a failed component. The system behavior is represented by the structure function $\varphi:\{0,1\}^n \rightarrow \{0,1\}$, where $\varphi(X)=1$ if the system functions and $\varphi(X)=0$ otherwise.

Definition 2.1: A coherent system is one whose structure function is monotone increasing and in which every component is relevant to system performance.

2.2 Minimal Path Sets

A path set is a subset of components whose successful operation guarantees system success. A minimal path set contains no proper subset having the same property. The family of minimal path sets completely characterizes successful operating configurations.

2.3 Minimal Cut Sets

A cut set is a subset of components whose simultaneous failure causes total system failure. A minimal cut set contains no proper subset that is itself a cut set. Minimal cut sets provide the dual representation of system reliability.

2.4 Reliability Polynomial

Assuming independent identical component reliability p, the system reliability is $R(p)=P(\varphi(X)=1)$. Expanding over all system states produces a polynomial $R(p)=\Sigma\ a_i\ p^i$ with integer coefficients determined solely by the system topology. Evaluating R(t) at an integer t produces a deterministic integer suitable for parameter generation.

2.5 Linear Diophantine Equations

A linear Diophantine equation has the form ax+by = c, where a, b and c are integers.

Theorem 2.1: The equation ax + by = c has an integer solution if and only if gcd (a, b) divides c.

Proof (outline): By Bézout's identity, integers u and v exist such that au+bv=gcd (a, b). Multiplying by c/gcd (a, b) yields a solution whenever gcd(a,b) divides c.

2.6 Bézout's Identity

For integers a and b there exist integers x and y satisfying ax+by=gcd(a,b). If gcd(a,b)=1, then ax+by=1. This identity provides the basis for modular inverse computation in RSA.

2.7 Extended Euclidean Algorithm

Given coprime integers e and φ(n), the Extended Euclidean Algorithm computes integers d and k satisfying ed−kφ(n)=1. Hence $d \equiv e^{-1} \pmod{\varphi(n)}$. The algorithm runs in O(log n) time.

2.8 Classical RSA Cryptosystem

Let p and q be distinct primes, n=pq and φ(n)=(p−1)(q−1). Choose e such that gcd(e,φ(n))=1. Compute d satisfying $ed \equiv 1 \pmod{\varphi(n)}$. Encryption is $C=M^e \bmod n$ and decryption is $M=C^d \bmod n$.

2.9 Mathematical Motivation for the Proposed Framework

Unlike conventional RSA, the proposed framework derives the public exponent from the integer evaluation of a reliability polynomial. Let $E_0=R(t)$, where t is a predetermined seed. The public exponent is selected as the smallest prime not less than $E_0 \bmod \varphi(n)$ that is coprime to φ(n). This provides deterministic, reproducible exponent generation while preserving the classical RSA security assumptions.

2.10 Illustrative Example I: Reliability Polynomial of a Redundant Alarm Subsystem

To make the constructions of Sections 2.1–2.4 concrete before they are used for cryptographic purposes, consider a small monitoring subsystem built from three components: two independently operating smoke detectors, x_1 and x_2, mounted in parallel so that either one alone is enough to register an event, and a single control relay, x_3, wired in series with the detector pair so that an alarm reaches the control panel only when the relay itself is working. The system is functioning, φ(X)=1, precisely when the relay is functioning and at least one detector is functioning.

The structure function follows directly from this description: $\varphi(X) = x_3[1-(1-x_1)(1-x_2)]$, which simplifies to $\varphi(X)=x_3(x_1 \vee x_2)$ because each $x_i \in \{0,1\}$. Checking all eight possible states of $X=(x_1,x_2,x_3)$ shows that the system functions only for the states (1,0,1), (0,1,1) and (1,1,1), and fails for the remaining five.

From this enumeration, the minimal path sets are {1,3} and {2,3}: removing either component from one of these pairs destroys the alarm function. The minimal cut sets are {3} and {1,2}: the relay alone is a single point of failure, whereas the two detectors must fail together before detection is lost. This pairing of a small path family with a small cut family is exactly the dual description promised in Sections 2.2 and 2.3.

Assume, as in Section 2.4, that every component operates independently with common reliability p. Since the detectors are in parallel, the probability that at least one of them is functioning is $1-(1-p)^2=2p-p^2$. As the relay is in series with this pair, the system reliability is the product $R(p)=p(2p-p^2)=2p^2-p^3$. Summing $p_k(1-p)^{(3-k)}$ directly over the three functioning states identified above reproduces this same expression term for term, confirming both the structure function and the polynomial.

For a numerical check, suppose each component carries a measured reliability of p=0.90 over its inspection interval, a plausible figure for a periodically tested detector or relay. Then R (0.90) = 2(0.81) − 0.729=1.620−0.729=0.891, so the subsystem is roughly 89.1% reliable noticeably below the 90% reliability of any single component, because the relay's series placement makes it the dominant point of failure identified by the minimal cut set {3}. Raising component reliability to p=0.95 lifts system reliability to R (0.95) = 2 (0.9025) − 0.857375=0.947625. The same integer-coefficient polynomial, evaluated here at a probability, is evaluated instead at an integer seed in Example II below to generate a cryptographic exponent.

2.11 Illustrative Example II: Deterministic Exponent Generation for a Five-Component Bridge Network

The second example carries the full construction of Sections 2.4–2.9 through to completion on the five-component bridge (Wheatstone) network referenced in the abstract, ending with a complete RSA key pair and the encryption and decryption of a sample message.

Consider a source node s and a sink node t joined through two intermediate nodes a and b, with component 1 on edge s–a, component 2 on edge a–t, component 3 on edge s–b, component 4 on edge b–t, and the bridging component 5 on edge a–b. This is the standard non-series-parallel topology used throughout the reliability literature precisely because it cannot be reduced to a combination of series and parallel blocks once component 5 is present [5], [6].

Enumerating all $2^5=32$ component states and testing s–t connectivity shows that the minimal path sets are {1,2}, {3,4}, {1,4,5} and {2,3,5}, and that the minimal cut sets are {1,3}, {2,4}, {1,4,5} and {2,3,5}. The bridge network is self-dual: the same four component subsets serve simultaneously as the minimal paths and the minimal cuts, a property noted for this topology in the classical reliability literature [5], [6].

Applying inclusion–exclusion over the four minimal path sets equivalently, summing $p^k(1-p)^{(5-k)}$ over the sixteen functioning states out of thirty-two gives the reliability polynomial $R(p)=2p^5-5p^4+2p^3+2p^2$. This four-term integer-coefficient polynomial is exactly the object required by Section 2.4 for deterministic parameter generation, and its coefficients (2,−5,2,2,0) depend only on the network topology, not on any probability assignment.

Following Section 2.9, fix the seed t=3. Evaluating the polynomial algebraically rather than probabilistically so that t need not lie in [0,1] gives $E_0=R(3)=2(3^5)-5(3^4)+2(3^3)+2(3^2)=2(243)-5(81)+2(27)+2(9)=486-405+54+18=153$.

For illustration at textbook scale, take the primes p=61 and q=53, so that the modulus is n=pq=3233 and Euler's totient is $\varphi(n)=(p-1)(q-1)=60\times52=3120$.

Reducing the seed value gives $E_0 \bmod \varphi(n) = 153 \bmod 3120 = 153$. Since $153=9\times17$ is composite, Section 2.9's rule advances through the successive integers: 154 is even and 155 is divisible by 5, so both share a factor with $\varphi(n)=2^4\cdot3\cdot5\cdot13$; 156 is again even. The integer 157 is prime and gcd (157, 3120) = 1, so the deterministic public exponent is e=157.

The private exponent is recovered, as in Section 2.7, by solving $157x-3120y=1$ with the Extended Euclidean Algorithm. The successive divisions are shown in Table 1.

Table 1: Extended Euclidean Algorithm applied to gcd (3120, 157).

Step	a	b	Quotient q	Remainder r (a = qb + r)
1	3120	157	19	137
2	157	137	1	20
3	137	20	6	17
4	20	17	1	3
5	17	3	5	2
6	3	2	1	1
7	2	1	2	0 (gcd = 1)

Back-substituting through these seven steps gives d=1093 as the coefficient of 157 in Bezout's identity, together with a corresponding coefficient of −55 for 3120. Direct verification confirms $157\ (1093) - 3120(55) = 171601-171600=1$, so $d\equiv e^{-1} \pmod{\varphi(n)}$ as required by Theorem 2.1 and the identity of Section 2.6.

Taking a representative plaintext block M=65 (M<n), encryption under the reliability-derived key gives $C=M^e \bmod n=65^{157} \bmod 3233=3086$. Decryption then recovers $M=C^d \bmod n=3086^{1093} \bmod 3233=65$, confirming the correctness of a key pair generated entirely from the reliability polynomial of the bridge network.

The example illustrates the central claim of Section 2.9: the reliability-theoretic seed does not weaken the classical RSA construction in any way. The exponent e=157 remains an ordinary admissible RSA public exponent, coprime to $\varphi(n)$ exactly as required by Section 2.8, and d=1093 remains its unique modular inverse. What changes is only the provenance of e, which is now traceable to a documented five-component network topology rather than to an arbitrary or conventionally fixed choice such as 65537, addressing the motivation set out in Section 1.1.

3. Related Work and Research Gap

This section surveys the mathematical literature relevant to the proposed reliability-theoretic RSA framework. It highlights prior work on RSA, Diophantine-equation-based cryptography, reliability theory, and deterministic parameter generation, and identifies the research gap addressed by the proposed method.

3.1 Classical Public-Key Cryptography

Since the introduction of public-key cryptography by Diffie and Hellman, RSA has remained one of the most influential asymmetric cryptosystems. Its security is based on the computational difficulty of factoring large composite integers. Numerous improvements have focused on implementation efficiency, padding, and key management, whereas the selection of the public exponent has typically remained fixed or arbitrary.

3.2 Diophantine Equations in Cryptography

Several researchers have investigated linear and nonlinear Diophantine equations for key exchange and public-key constructions. These schemes employ integer solutions of algebraic equations as cryptographic secrets. Although mathematically interesting, most introduce alternative hardness assumptions rather than preserving the classical RSA framework. In contrast, the present work uses a linear Diophantine equation only to compute the modular inverse, retaining RSA's original security assumption.

3.3 Reliability Theory and Coherent Systems

Reliability theory provides rigorous mathematical tools for analysing engineering systems using structure functions, minimal path sets, minimal cut sets, and reliability polynomials. These combinatorial invariants have been extensively studied for performance evaluation and fault tolerance, but have received little attention as deterministic sources of cryptographic parameters.

3.4 Research Gap

Existing RSA implementations do not provide an auditable mathematical provenance for the public exponent, while existing reliability-theoretic studies do not connect combinatorial reliability invariants with public-key cryptography. Likewise, Diophantine cryptographic schemes generally replace RSA rather than complementing it. This leaves an opportunity to develop a deterministic exponent-generation framework that integrates reliability theory with the established RSA architecture.

3.5 Novelty of the Proposed Work

The proposed framework contributes: (i) deterministic generation of the RSA public exponent from a reliability polynomial; (ii) explicit interpretation of RSA key generation through a linear Diophantine equation and Bézout's identity; (iii) reproducible parameter generation linked to an engineering topology; and (iv) preservation of the classical factorization-based security model.

3.6 Comparison with Existing Approaches

Approach	Primary Mathematics	Security Basis	Parameter Origin
Classical RSA	Number Theory	Integer Factorization	Fixed/Chosen Exponent
Diophantine Schemes	Diophantine Equations	Alternative Algebraic Problems	Equation Solutions
Reliability Analysis	Combinatorics	Not Cryptographic	Reliability Polynomial
Proposed RT-RSA	Reliability + Number Theory	Integer Factorization	Deterministic Reliability Polynomial

3.7 Concluding Remarks

The literature indicates that reliability theory, RSA, and Diophantine equations have evolved largely independently. The proposed framework bridges these domains by introducing a mathematically reproducible exponent-generation mechanism while preserving the well-established RSA cryptosystem.

References

[1] W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644–654, 1976.
[2] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120–126, 1978.
[3] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL: CRC Press, 1996.
[4] I. Niven, H. S. Zuckerman, and H. L. Montgomery, An Introduction to the Theory of Numbers, 5th ed. New York: Wiley, 1991.
[5] R. E. Barlow and F. Proschan, Statistical Theory of Reliability and Life Testing: Probability Models. New York: Holt, Rinehart and Winston, 1975.
[6] M. Rausand and A. Høyland, System Reliability Theory: Models, Statistical Methods, and Applications, 2nd ed. Hoboken, NJ: Wiley, 2004.
[7] J.-L. Marichal, "Structure functions and minimal path sets," IEEE Transactions on Reliability, vol. 65, no. 2, pp. 763–768, 2016.
[8] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM Journal on Computing, vol. 26, no. 5, pp. 1484–1509, 1997.
[9] Chaya Kumari Divakarla1, R. Ajitha, Sonam Kumar, N. Vijaya, Supriya B J"Construction of a Public-Key Cryptosystem Using Dominating Interior Polynomials of Fuzzy Graphs: A Novel Knapsack-Type Scheme with Encryption and Decryption Algorithms"
[10] Chaya Kumari Divakarla, R. Ajitha, Hymavathi, Vinoda Lakshmi, "Dominating Polynomial of Graphs in Asymmetric Key Cryptosystem Construction: An Algorithm and Illustrative Example"