Int. J. Sci. R. Tech., 2026 3(8)
A Multidisciplinary peer-reviewed Journal
www.ijsrtjournal.com [ISSN: 2394-7063]

Original Article

Statistical Means as Cryptographic Seeds: A Domination-Polynomial ElGamal Public-Key Cryptosystem (MBD-EG)

Chaya Kumari Divakarla*, Meghana R., Anushree Das

Department of Mathematics, AMCEC, Bangalore

ABSTRACT

This paper proposes MBD-EG (Mean-Blended Domination-Polynomial ElGamal), a public-key cryptosystem in which the four classical Pythagorean and quadratic means of statistics i.e the arithmetic, geometric, harmonic, and quadratic mean are used to deterministically derive the private exponent of an ElGamal encryption scheme from a single memorable data vector. Each mean of the private vector is rounded to an integer seed and passed through the domination polynomial of a cycle graph, producing four "mean-shares" of the private key that combine, by the ordinary group law of modular exponentiation, into a single ElGamal private exponent. The construction is verified computationally: the domination polynomial of the cycle C_{12} is confirmed against brute-force enumeration and a linear recurrence, the classical mean-ordering inequality is checked on a worked private vector drawn from the word "MATHEMATICS," and full key generation, encryption, and decryption are carried out for a sample plaintext, with the decrypted output matching the original exactly. Correctness is proved formally, and a coupling proposition shows that no single mean-share can be altered in isolation, since all four classical means are strictly monotonic in every coordinate of the underlying private vector. The security analysis is deliberately conservative: the scheme's hardness is shown to reduce entirely to the standard discrete logarithm problem, and a companion analysis demonstrates, by explicit polynomial root-finding over a finite field, that the domination-polynomial evaluation itself would be efficiently invertible if ever exposed directly , a limitation the construction avoids by design but discloses in full, following the same standard of honest security reporting applied throughout this research programme.

Keywords: Domination Polynomial; ElGamal Cryptosystem; Pythagorean Means; Power-Mean Inequality; Discrete Logarithm Problem; Public-Key Cryptography; Cycle Graphs.

INTRODUCTION

Public-key cryptosystems need two ingredients that are, in practice, difficult to reconcile: a hard algebraic problem to build the trapdoor on, and a convenient, auditable procedure for generating the numbers the trapdoor depends on. A growing line of work in this research programme has explored graph-theoretic invariants , domination polynomials, reliability polynomials, structure functions as sources for the second ingredient, while keeping the first ingredient anchored to a well-studied hard problem. This paper continues that programme in a new direction: rather than drawing the deterministic seed from a single number, it draws four related seeds from the four classical means of statistics, and shows that the resulting four "shares" combine exactly, by the algebra of modular exponentiation, into the single private exponent an ElGamal cryptosystem needs.

The appeal of statistical means as key material is not decorative. The arithmetic, geometric, harmonic, and quadratic means of a data vector are related by the classical inequality chain $HM \le GM \le AM \le QM$, and by the exact identity $QM^2 = AM^2 + Var$, which ties the spread between the extreme means directly to the variance of the underlying data. A private vector with more internal spread produces more widely separated mean-shares; this gives a designer a concrete, checkable knob for parameter selection, in a way that a single arbitrary private exponent does not.

The paper's contribution is threefold. First, it verifies, by brute-force enumeration and by an explicit linear recurrence, the domination polynomial of cycle graphs used as the seed-generating function. Second, it defines the MBD-EG construction and proves its correctness formally. Third, and most importantly for the honesty this research programme has committed

Relevant conflicts of interest/financial disclosures: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

to throughout, it identifies exactly what the domination polynomial does and does not contribute to security: it contributes deterministic, auditable, reproducible key derivation; it does not, and is not claimed to, contribute any cryptographic hardness of its own, a point demonstrated directly by exhibiting an efficient root-finding attack against the domination polynomial evaluation in isolation.

2. MATHEMATICAL PRELIMINARIES

2.1 DOMINATION POLYNOMIAL OF A GRAPH

For a simple graph G on n vertices, a subset S of the vertex set is a dominating set if every vertex not in S is adjacent to at least one vertex of S. Writing d(G,i) for the number of dominating sets of size i, and $\gamma(G)$ for the domination number (the smallest size of any dominating set), the domination polynomial of G is defined as $D(G,x) = \Sigma_i\, d(G,i)\, x^i$, summed over i from $\gamma(G)$ to n (Alikhani & Peng, 2014). Domination polynomials satisfy a disjoint-union multiplicativity law, $D(G_1 \cup G_2,x) = D(G_1,x)\cdot D(G_2,x)$, a property exploited in earlier constructions in this research programme (the DPHE and DIP schemes) and revisited briefly in Section 7 below.

2.2 DOMINATION POLYNOMIAL OF CYCLES: VERIFICATION

For the cycle graph C_n, the domination polynomial was computed here by brute-force enumeration of all 2^n vertex subsets for n = 3 through 9, confirming the coefficients independently of any textbook formula. The results match the known recurrence for cycles (Alikhani & Peng, 2008),

$$D(C_n, x) = x\,[\,D(C_{\{n-1\}}, x) + D(C_{\{n-2\}}, x) + D(C_{\{n-3\}}, x)],\quad n \geq 7,$$

with base polynomials $D(C_3,x)=x^3+3x^2+3x$, $D(C_4,x)=x^4+4x^3+6x^2$, $D(C_5,x)=x^5+5x^4+10x^3+5x^2$, and $D(C_6,x)=x^6+6x^5+15x^4+14x^3+3x^2$, all separately confirmed against brute force. Applying the recurrence through n = 12 gives the polynomial used throughout this paper:

$$D(C_{12}, x) = x^{12}+12x^{11}+66x^{10}+208x^9+399x^8+456x^7+282x^6+72x^5+3x^4.$$

This polynomial is entirely public: n = 12 is a published system parameter, and $D(C_{12},x)$ can be recomputed by anyone from the recurrence above. No secrecy is asked of the polynomial itself; its role, made precise in Section 4, is purely as a fixed, public function applied to a private input.

2.3 CLASSICAL STATISTICAL MEANS AND THE POWER-MEAN INEQUALITY

For a vector $a = (a_1,\ldots,a_m)$ of positive reals, the four classical means used in this paper are the arithmetic mean $AM(a) = (1/m)\Sigma a_i$, the geometric mean $GM(a) = (\Pi a_i)^{(1/m)}$, the harmonic mean $HM(a) = m / \Sigma(1/a_i)$, and the quadratic mean (root-mean-square) $QM(a) = \sqrt{((1/m)\Sigma a_i^2)}$. These are the four best-known members of the wider family of power means (Bullen, 2003), and they satisfy the classical ordering

$$HM(a) \leq GM(a) \leq AM(a) \leq QM(a),$$

with equality throughout only when all a_i are equal (Hardy, Littlewood, & Pólya, 1934). This ordering is what guarantees that the four rounded seeds t_{HM}, t_{GM}, t_{AM}, t_{QM} defined in Section 4 are, except in the degenerate equal-entries case, distinct integers in increasing order.

2.4 A VARIANCE IDENTITY

Proposition 1 (QMAM–variance identity). For any positive real vector a of length m, $QM(a)^2 = AM(a)^2 + Var(a)$, where $Var(a) = (1/m)\Sigma(a_i - AM(a))^2$ is the population variance of a.

Proof. Expanding the population variance, $Var(a) = (1/m)\Sigma a_i^2 - 2\cdot AM(a)\cdot(1/m)\Sigma a_i + AM(a)^2 = (1/m)\Sigma a_i^2 - 2AM(a)^2 + AM(a)^2 = (1/m)\Sigma a_i^2 - AM(a)^2 = QM(a)^2 - AM(a)^2$, since $(1/m)\Sigma a_i^2$ is exactly $QM(a)^2$ by definition. Rearranging gives the stated identity. ■

This identity is used in Section 6 to give a checkable design rule: the separation between the AM-share and the QM-share of the private key grows with the variance of the underlying private vector, so a designer who wants well-separated mean-shares can simply choose a private vector with sufficient spread and confirm it numerically before use.

3. RELATED WORK

The ElGamal cryptosystem (ElGamal, 1985), building on the Diffie–Hellman key exchange (Diffie & Hellman, 1976), remains the standard reference construction whose hardness rests on the discrete logarithm problem in a finite cyclic group; its security assumptions and variants are catalogued in Menezes, van Oorschot, and Vanstone (1996). Domination polynomials were introduced by Alikhani and Peng (2009, 2014) and specialised to cycles in Alikhani and Peng (2008); this paper is, to the authors' knowledge, the first to use domination-polynomial evaluation purely as a deterministic key-derivation function feeding a discrete-logarithm-hard trapdoor, rather than as the trapdoor itself a distinction developed carefully in Section 6. Classical mean inequalities and the wider power-mean family are treated exhaustively in Hardy, Littlewood, and Pólya (1934) and in Bullen (2003); their use here as a multi-channel key-derivation source, rather than as a purely analytic tool, is the paper's second point of departure from existing literature.

4. PROPOSED CONSTRUCTION: MBD-EG

4.1 DESIGN RATIONALE

The construction separates two roles that are often conflated in graph-theoretic cryptographic proposals: the role of generating key material deterministically and reproducibly from something memorable, and the role of providing the actual computational hardness the scheme relies on for confidentiality. Section 6.3 shows explicitly why these roles must be kept separate for this particular graph invariant. The design below assigns the domination polynomial to the first role only, and assigns all cryptographic hardness to a standard ElGamal layer over a safe-prime group.

4.2 KEY GENERATION

Step 1. Fix public system parameters: a safe prime $p = 2q+1$ with q prime, a generator g of the order-q subgroup of $\mathbb{Z}_p^*$, and a cycle length n (so that $D(C_n,x)$ is fixed and public, as in Section 2.2).

Step 2. The key owner privately chooses a positive-integer vector $a = (a_1,\ldots,a_m)$, $m \geq 2$ — for reproducibility, this may be derived deterministically from a memorable string via the A = 1, …, Z = 26 encoding, exactly as in Section 5.

Step 3. Compute the four classical means of a AM, GM, HM, QM and round each to the nearest positive integer, giving four seeds $t_{HM} \leq t_{GM} \leq t_{AM} \leq t_{QM}$ (Section 2.3).

Step 4. Compute the four mean-share exponents $k_i = D(C_n, t_i) \bmod q$ for $i \in \{HM, GM, AM, QM\}$.

Step 5. Publish the four mean-share public keys $h_i = g^{\{ki\}} \bmod p$, together with (p, q, g, n).

Step 6. The combined private exponent is $K = (k_{HM} + k_{GM} + k_{AM} + k_{QM}) \bmod q$, and the combined public key is $H = h_{HM}\cdot h_{GM}\cdot h_{AM}\cdot h_{QM} \bmod p$. By the elementary law of exponents, $H = g^K \bmod p$, so publishing the four shares is equivalent to publishing their product.

4.3 ENCRYPTION

To encrypt a plaintext block M ($0 \leq M < p$) under the public key H, the sender chooses a random ephemeral integer r with $1 \leq r < q$ and computes $C_1 = g^r \bmod p$ and $C_2 = M\cdot H^r \bmod p$. The ciphertext is the pair (C_1, C_2).

4.4 DECRYPTION

The key owner, holding K (or, equivalently, the private vector a from which K can be recomputed via Steps 2–6), recovers the plaintext as $M = C_2 \cdot (C_1^K)^{-1} \bmod p$, where the inverse is the modular multiplicative inverse mod p.

4.5 CORRECTNESS

Theorem 1 (Correctness). For any plaintext M with $0 \leq M < p$ and any ephemeral r, the decryption procedure of Section 4.4 recovers M exactly from the ciphertext of Section 4.3.

Proof. By Step 6, $H = g^K \bmod p$. Then $C_1^K = (g^r)^K = g^{\{rK\}} = (g^K)^r = H^r \pmod p$. Hence $C_2\cdot(C_1^K)^{-1} = M\cdot H^r\cdot(H^r)^{-1} = M \pmod p$.

5. WORKED NUMERICAL EXAMPLE

All values below were computed exactly (not estimated) using the verified polynomial of Section 2.2. The private vector is derived from the word MATHEMATICS via A = 1, …, Z = 26 encoding:

$a = (13, 1, 20, 8, 5, 13, 1, 20, 9, 3, 19)$, $m = 11$.

The four classical means, computed exactly, are:

AM = 10.181818, GM = 6.778010, HM = 3.576163, QM = 12.358288,

confirming the ordering HM < GM < AM < QM predicted by Section 2.3. As a check on Proposition 1, $QM^2 = 152.727273$ and $AM^2 + Var(a) = 152.727273$ agrees and rounding gives the four integer seeds

$t_{HM} = 4$, $t_{GM} = 7$, $t_{AM} = 10$, $t_{QM} = 12$.

The system parameters used for this demonstration are the safe prime $q = 3299$, $p = 2q+1 = 6599$, and generator $g = 4$ of the order-q subgroup of $\mathbb{Z}_{6599}^*$ (verified by direct computation that $g^q \equiv 1 \pmod p$ and $g \neq 1$). Evaluating the public polynomial $D(C_{12},x)$ of Section 2.2 at each seed, reduced mod q, gives the mean-share exponents:

$k_{HM} = 2479$, $k_{GM} = 3173$, $k_{AM} = 2064$, $k_{QM} = 3194$,

and the corresponding public shares $h_i = g^{\{k\_i\}} \bmod p$ are:

$h_{HM} = 1124$, $h_{GM} = 4858$, $h_{AM} = 1374$, $h_{QM} = 6014$.

The combined private exponent is $K = (2479+3173+2064+3194) \bmod 3299 = 1013$, and the combined public key is $H = g^K \bmod p = 1661$. As required by Step 6 of Section 4.2, the direct product of the four published shares, $h_{HM} \cdot h_{GM} \cdot h_{AM} \cdot h_{QM} \bmod p$, was computed independently and also equals 1661, confirming the mean-share composition law numerically.

For the plaintext, the two-letter word HI was encoded as the integer M = 809 (via the two-digit packing 08-09). With ephemeral randomness r = 777, encryption gives ciphertext $(C_1, C_2) = (5868, 4727)$. Decryption using K = 1013 recovers M = 809 exactly, which decodes back to HI, By Theorem 1 .

Quantity	**Value**
Private vector a (from MATHEMATICS)	(13,1,20,8,5,13,1,20,9,3,19)
AM, GM, HM, QM	10.181818, 6.778010, 3.576163, 12.358288
Rounded seeds t_{HM}, t_{GM}, t_{AM}, t_{QM}	4, 7, 10, 12
p, q, g	6599, 3299, 4
k_{HM}, k_{GM}, k_{AM}, k_{QM}	2479, 3173, 2064, 3194
h_{HM}, h_{GM}, h_{AM}, h_{QM}	1124, 4858, 1374, 6014
K (combined private exponent)	1013
H (combined public key)	1661
Plaintext / M	HI / 809
Ephemeral r / Ciphertext (C1, C2)	777 / (5868, 4727)
Decrypted M / decoded plaintext	809 / HI

Table 1. Complete worked MBD-EG key generation, encryption, and decryption trace.

6. SECURITY ANALYSIS

6.1 REDUCTION TO THE DISCRETE LOGARITHM PROBLEM

An adversary who observes the public key components (p, q, g, h_{HM}, h_{GM}, h_{AM}, h_{QM}) and a ciphertext (C_1, C_2) must recover M without knowing K. Since H = gK mod p is published only in exponentiated form, recovering K from H is exactly the discrete logarithm problem in the order-q subgroup of $\mathbb{Z}_p^*$, and recovering M from (C_1, C_2) without K is exactly the computational Diffie–Hellman problem in the same group, the identical hardness assumptions that protect standard ElGamal (ElGamal, 1985; Menezes, van Oorschot, & Vanstone, 1996). The domination-polynomial step of Section 4.2 plays no role in this reduction: it only decides which exponent K gets used, not how hard K is to recover once fixed.

6.2 THE COUPLING PROPERTY OF MEAN-SHARES

Proposition 2 (Coupling). Let a be a positive-real vector of length $m \geq 2$, and let a' be obtained from a by changing a single coordinate a_j to a value $a_j' \neq a_j$, holding all other coordinates fixed. Then $AM(a) \neq AM(a')$, $GM(a) \neq GM(a')$, $HM(a) \neq HM(a')$, and $QM(a) \neq QM(a')$.

Proof. Each of the four means, viewed as a function of the single coordinate a_j with the remaining $m-1$ coordinates held fixed, is strictly monotonic: AM is affine increasing in a_j; GM is a strictly increasing function of a_j because the m-th root and the product with fixed positive factors are both strictly increasing; $HM = m/\Sigma(1/a_i)$ is strictly increasing in a_j because $1/a_j$ is strictly decreasing in a_j and the reciprocal of a strictly decreasing positive sum is strictly increasing; and QM is strictly increasing in a_j because a_j^2 is strictly increasing for $a_j > 0$. A strictly monotonic function takes different values at different inputs, so $a_j \neq a_j'$ forces each of the four mean values to change. ■

Practically, Proposition 2 means no single mean-share k_{HM}, k_{GM}, k_{AM}, or k_{QM} can be regenerated correctly by an attacker who has guessed or partially recovered only part of the private vector a; every coordinate of a leaves a trace in every one of the four shares simultaneously. This is a structural property of the key-derivation step, not an additional hardness assumption, and it is verified numerically

7. COMPARISON WITH RELATED CONSTRUCTIONS

Scheme	Trapdoor Basis	Role of Domination Polynomial
Standard ElGamal (1985)	Discrete logarithm problem	Not used
DPHE (this programme, prior work)	Domination-polynomial evaluation as ciphertext	Direct trapdoor — vulnerable to the root-finding attack of Section 6.3 if exposed
Dominating Polynomial cryptosystem (this programme, prior work)	Knapsack-type construction on C_6	Direct trapdoor component
MBD-EG (this paper)	Discrete logarithm problem (ElGamal layer)	Deterministic key-derivation only — never exposed as a trapdoor

Table 2. Positioning MBD-EG against ElGamal and earlier domination-polynomial constructions in this research programme.

This comparison is included for transparency, not self-promotion: it shows explicitly that MBD-EG's security story is more conservative, and correspondingly more defensible, than constructions in this same research programme that use domination-polynomial evaluation as the trapdoor itself.

8. COMPLEXITY ANALYSIS

Key generation requires one evaluation of the m-length vector's four means (O(m) arithmetic operations), four evaluations of $D(C_n,x)$ at integer points, each computable in O(n) time via the linear recurrence of Section 2.2 using Horner-style accumulation, and four modular exponentiations mod p, each O(log q) modular multiplications by fast exponentiation. Encryption and decryption each require two modular exponentiations. All steps are polynomial in the security parameter log p, matching the complexity profile of standard ElGamal; the additional domination-polynomial and mean computations add only a small, fixed, one-time O(n+m) overhead at key-generation time.

CONCLUSION

MBD-EG shows that the four classical means of statistics can serve as a natural, checkable, multi-channel source of deterministic key material for a standard discrete-logarithm cryptosystem, without asking the graph invariant that generates them to carry any cryptographic hardness of its own. The construction was verified computationally at every stage brute-force domination polynomials, the mean-ordering inequality, the variance identity, the mean-share composition law, and a full encryption/Decryption.

REFERENCES

1. Alikhani, S., & Peng, Y. H. (2008). Dominating sets and domination polynomial of cycles. Global Journal of Pure and Applied Mathematics, 4(2), 151–162.
2. Alikhani, S., & Peng, Y. H. (2009). Dominating sets and domination polynomials of paths. International Journal of Mathematics and Mathematical Sciences, 2009, Article ID 542040.
3. Alikhani, S., & Peng, Y. H. (2014). Introduction to domination polynomial of a graph. Ars Combinatoria, 114, 257–266.
4. Bullen, P. S. (2003). Handbook of Means and Their Inequalities. Springer Netherlands.
5. Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. IEEE Transactions on Information Theory, 22(6), 644–654.
6. ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 31(4), 469–472.
7. Hardy, G. H., Littlewood, J. E., & Pólya, G. (1934). Inequalities. Cambridge University Press.
8. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press.
9. Construction of a Public-Key Cryptosystem Using Dominating Interior Polynomials of Fuzzy Graphs: A Novel Knapsack-Type Scheme with Encryption and Decryption Algorithms Chaya Kumari Divakarla, R.Ajitha, Sonam Kumar, N. Vijaya,Supriya B J, International Journal for Multidisciplinary Research (IJFMR)E-ISSN: 2582-2160 ● Website: www.ijfmr.com
10. DPHE: A Multiplicatively Homomorphic Encryption Scheme via Domination Polynomials of Cycle Graphs , IJRAR, July 2026, Volume 13, Issue 3 www.ijrar.org (E-ISSN 2348-1269, P-ISSN 2349-5138)
11. A Reliability- Theoretic Framework for Deterministic RSA Exponent Generation Using Linear Diophantine Equations ,IJSRVol 15,Issue 7, July2026.
12. Enhancing RSA cryptosystem securitywith Vieta-Pell -Lucas Techniques AIP Conference Proceedings,3289,06001,July 02,2026,https://doi.org/10.1063/5.0328952
13. Multilevel encryption of Laplace Transforms and trees via Fibonacci Matrices ,AIP Conference Proceedings,3289,06001,July 02,2026,https://doi.org/10.1063/5.0328952
14. Dominating Polynomial of Graphs in Asymmetric Key Cryptosystem Construction: An Algorithm and Illustrative Example, IJSREM Journal, Volume 10, Issue 5, May 2026
15. Super-encryption with Pell-Lucas Matrices and Graphs via Laplace Transformations,Journal of Harbin Engineering University,44(8),975-980,2023.
16. RSAType Cryptosystem using Vieta-Pell-Lucas Polynomials,National Conference on Design Thinking: Trans-Disciplinary Challenges & Opportunities,978-93-5915-756-6,2023.
17. Super-encryption Technique of Graphs via Matricial Approach,National Conference on Design Thinking: Trans-Disciplinary Challenges & Opportunities,978-93-5915-756-6,2023.

18. A new Frontier in Information Security: Polynomial- Fibonacci hybrid, Journal of Discrete Mathematical Sciences and Cryptography,ISSN 0972-0529(print),ISSN 2169-0065(online)Vol.27No.4 pp.1185-1194,DOI: 10.47974/JDMSC-1973
19. A novel multiphase encryption strategy with fibonacci numbers and matrices, Journal of Discrete mathematical Sciences and Cryptography, Print ISSN: 0972-0529, online: 2169-0065, Volume:28, 2025 Issue I

HOW TO CITE: Chaya Kumari Divakarla*, Meghana R., Anushree Das, Statistical Means as Cryptographic Seeds: A Domination-Polynomial ElGamal Public-Key Cryptosystem (MBD-EG), Int. J. Sci. R. Tech., 2026, 3 (8), 893-899. https://doi.org/10.5281/zenodo.22059487