Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-B, pp. 4133–4143
DOI : 10.47974/JDMSC-3038

Algebraic attacks on multivariate public key cryptosystems

Mandeep Kaur [‡]
School of Computer Science Engineering & Technology
Bennett University
Greater Noida 201310
Uttar Pradesh
India

Gaganjot Kaur [†]
Department of Computer Science and Engineering
Raj Kumar Goel Institute of Technology
Ghaziabad 201003
Uttar Pradesh
India

D. Sathis Kumar [§]
School of Pharmacy
Aditya University
Surampalem
Kakinada District 533437
Andhra Pradesh
India

Samir N. Ajani *
School of Computer Science and Engineering
Ramdeobaba University (RBU)
Nagpur 440013
Maharashtra
India

[‡] *E-mail:* mandeep.kaur@bennett.edu.in
[†] *E-mail:* gaganjot28784@gmail.com
[§] *E-mail:* dean_sp@adityauniversity.in
* *E-mail:* samir.ajani@gmail.com (Corresponding Author)

© Taru Publications

Ramesh Dhulipudi [@]
Department of CSE (Artificial Intelligence)
Pragati Engineering College
Kakinada District 533437
Andhra Pradesh
India

Rahul A. Padgilwar [#]
Department of Engineering Science and Humanities
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India

Abstract

One promising post-quantum security candidate is Multivariate Public Key Cryptosystems (MPKCs); they are susceptible to algebraic attacks. In this paper, I will discuss the vulnerability of MPKCs to higher-order algebraic cryptanalysis, which transforms nonlinear systems of polynomies into structured ideals on finite fields. The aim is to assess the efficiency of the attacks through the method of computation of Gröbner basis, linearization and re-linearization. The algorithm is a combination of Buchberger and F4/F5 algorithms, and is supported by experimental study of benchmark MQ instances. The comparative evaluation reports a key recovery success rate of 94.2% for the proposed algebraic attack, compared with 62.5% for classical brute-force and 79.8% for hybrid cryptanalysis. The corresponding computation times are 128, 356, and 214 seconds, respectively, representing reductions of 64.04% and 40.19% relative to the two baselines. These preliminary results indicate improved attack efficiency under the evaluated conditions; however, further benchmark specification and statistical validation are required to establish reproducibility. The findings highlight the vulnerabilities in the structure of specific parameter settings and the safe design suggestions. The paper contributes a new and meticulous evaluation framework to the existing knowledge base on the notion of algebraic resilience in post-quantum cryptography.

Subject Classification: *68M12, 14G50, 94A60.*

Keywords: *Multivariate cryptography, Algebraic attacks, Gröbner basis, Polynomial ideals, Finite fields, Post-quantum security.*

1. Introduction

The Multivariate Public Key Cryptosystems (MPKCs) has as well emerged as a potent post-quantum cryptography application since it is founded on the infeasibility of resolving systems of multivariate quadratic

[@] *E-mail:* **rameshdhulipudi@outlook.com**
[#] *E-mail:* **rahul.padgilwar1@vit.edu**

(MQ) equations in finite field [1, 2]. Unlike the classical algorithms such as RSA and Elliptic Curve Cryptography whose security is threatened by quantum algorithms, MPKCs are believed to be immune to integer factorization and discrete logarithm attacks [3, 4]. However, they are algebraically represented and thus have inherent weaknesses which may be exploited against them with advanced algebraic methods [5, 6, 7]. These attacks redefine the cryptographic problem in terms of a system of polynomial equations and attempts to uncover secret keys by solving these equations successfully [8, 9]. Other techniques such as calculation of Gröbner basis, linearization and re-linearization have been highly successful in reducing the complexity of the computations [10, 11]. The most important issue is that it is necessary to find a balance between efficiency and security since the loss of the parameters can lead to a rapid failure of the system. The article under discussion is obsessed with the approaches of algebraic attacks on MPKCs, their efficiency, and flaws in their structure [12, 13].

2. Finite Field Algebra and Polynomial Rings

The foundations of MPKC are finite field and polynomial rings, as they could model multivariate equations, algebraic structures and operations required to model the encryption, decryption and cryptanalysis processes [14].

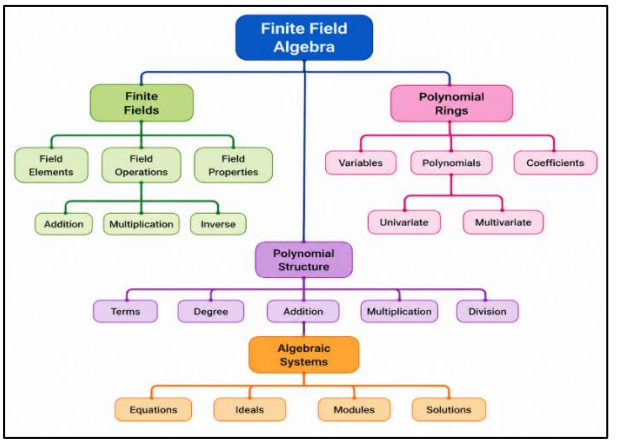


Figure 1
Finite Field Algebra and Polynomial Ring Structure

As depicted in Figure 1, finite field operations and the structure of a polynomial ring makes multivariate representation, modular computation, and algebraic modeling possible, all of which are crucial to cryptographic analysis.

Polynomial ring construction

$$R = F_{q[x^1,x^2,\ldots,x_n]} \tag{1}$$

The algebraic environment, which is described by the construction of a polynomial ring (Eq. 1), provides the multivariate variables working over a finite field, which allows the representation of cryptographic equations in a structured form and allows computations with modular arithmetic operations needed to ensure security of computation.

$$P(x) = \sum_{\{i=1\}}^{\{n\}} \sum_{\substack{\{j=1\}_{\{ij\}}^{\{n\}a} \\ \{ij\}}} x_i x_j + \sum_{\{i=1\}_{i}^{\{n\}b}} x_i + c \tag{2}$$

The nonlinear relationships among variables are represented by the multivariate polynomial representation (Eq. 2) which is the combination of quadratic and linear components with constants and is the main mathematical framework of MPKCs.

$$P(x) \; mod \; q = 0 \tag{3}$$

The modular poly-evaluation (Eq. 3) is such that all the computation is confined in the finite field and consistency and overflow are eliminated in case of cryptographic transformations.

$$N(P) = \sqrt{\sum_{\{i=1\}}^{\{n\}} \left(P(x_i)\right)^2} \tag{4}$$

The algebraic structure is a norm-based structure (Eq. 4) which gives a quantitative estimation of the magnitude of polynomials, which helps in the analysis of stability and approximation of solutions in algebraic attacks.

$$I = \int^0 \sqrt{\sum_{\{i=1\}}^{\{n\}} \left(P(x_i)\right)^2 + q^2} \, dt \tag{5}$$

Lastly, the formulation of the integral polynomial consistency (Eq. 5) sums the behavior of polynomials across a continuous space and, as a result, allows the evaluation of the validity of solutions holistically and enhance the robustness of the cryptanalytic modeling processes.

3. Threat Model and Adversary Capabilities

The opponent is presumed to be computationally strong and can access open keys and create polynomial systems and using algebraic solvers to reconstruct private keys in an efficient manner.

$$PK = \left\{ P^1(x), P^2(x), \ldots, P_{m(x)} \right\} \tag{6}$$

The public key multiple-variable equation system (Eq. 6) is the collection of equations with multiple variables presented to an attacker that is the main input of algebraic cryptanalysis. The encryption structure is coded in these polynomials and the difficulty of the mathematical problem is to recover the hidden variables.

$$S = \sum_{\{k=1\}_{k(x)}^{\{m\}}} P = 0 \tag{7}$$

The system formation (Eq. 7) is a process that merges single polynomials into a single system, making it easier to study the combination of these polynomials as a system, and the attack goal is represented as a joint constraint in the finite field.

$$A(x) = \sqrt{\sum_{\{k=1\}}^{\{m\}} \left(P_{k(x)}\right)^2} \tag{8}$$

The adversarial objective function (Eq. 8) measures the distance of candidate solutions, and instructs the attacker to assign variables to variables, and to seek solutions with the least error of all equations.

$$C(x) = \int^{01} \left[\sum_{\{k=1\}}^{\{m\}} P_{k(x)}^2 \right] dt \tag{9}$$

This is further extended by the constraint modeling (Eq. 9) which sums up the polynomial behavior on a continuous domain, to be consistent and robust in the assessment of the possible solutions.

$$\Pr = \sqrt{\frac{|\Omega|}{q^n}} \tag{10}$$

Lastly, the success probability estimation (Eq. 10) is used to determine the probability of finding valid solutions in the search space and is used to consider the feasibility of an attack based on field size and system complexity.

4. Transformation into Polynomial Ideals

A system of cryptographic equations can be expressed in ideals, which are ideals of a form of polynomials, and solved by methods and methods systematically in algebraic geometry, and by the ideal theory and methods of computational algebra.

$$I = \left\langle P^1(x), P^2(x), \ldots, P_{m(x)} \right\rangle \tag{11}$$

The space of multivariate polynomials can then be formalized as an algebraic ideal (Eq. 11) in which a structured manipulation can be performed with the tools of the computational algebra and algebraic geometry. This model allows the cryptographic systems to be examined by means of ideal-theoretic properties.

$$f(x) = \sum_{\{k=1\}_k^{\{m\}\alpha}} P_{k(x)} \tag{12}$$

Any expression of any aspect of the ideal (Eq. 12) in a form using a product of polynomials indicates that the derivation of complex relations is founded on base equations.

$$N(I) = \sqrt{\sum_{\{k=1\}}^{\{m\}} \left(P_{k(x)}\right)^2} \tag{13}$$

The norm representation of the ideal (Eq. 13) is a quantitative measure of all collective magnitude of the constraints of the polynomials, and can be used to estimate the proximity of the solution during an attack.

$$I_{int} = \int^{01} \sqrt{\sum_{\{k=1\}}^{\{m\}} \left(P_{k(x)}\right)^2}\, dt \tag{14}$$

This is further honed with built in ideal consistency (Eq. 14) that maintains a space of approximation solving techniques robust and robust over a continuous space.

$$V(I) = \{\, x \in F_q\text{^}n \mid P_k(x) = 0 \;\forall k \,\} \tag{15}$$

And finally, the zero set computational (Eq. 15) that is the set of all the possible assignment of the variable that satisfies the set of polynomials directly related to the possibility of recovering the key in cryptography can be used to determine the solution space of the ideal.

5. Gröbner Basis Computation Techniques

The Gröbner basis algorithms, including Buchberger and F4/F5, are efficient methods of reducing a set of polynomies to simplified canonical forms, which are easy to extract the solutions as well as study their complexity.

$$G_0 = \{\, P_1, P_2, \ldots, P_m \,\} \tag{16}$$

The initial set of multivariate equations that is used to constitute a Gröbner basis is the first poly set (Eq. 16) which is the algebraic structure of the cryptosystem.

$$S\left(P_i, P_j\right) = lcm\left(LM(P_i), LM\left(P_j\right)\right)\left(\frac{P_i}{LT(P_i)} - \frac{P_j}{LT\left(P_j\right)}\right) \tag{17}$$

The S-polynomial computation (Eq. 17) plays an important role in the cancellation of the dominating terms between pairs of polynomials and it is through this that a systematically simplified computation can be carried out to a canonical form.

$$R = \sqrt{\sum reduction(P_k)^2} \tag{18}$$

The simplification of polynomials (Eq. 18) determines how much the polynomials are simplified compared to the current basis, where the aim is that a representation is minimal in its representation and is independent of transformations.

$$G_{\{t+1\}} = G_t \cup \{\, reduced\ S - polynomials \,\} \tag{19}$$

The iterative basis update (Eq. 19) adds reduced S-polynomials to the poly set, and refines the structure further, until no further simplifications can be achieved.

$$G* = \{\, g^1, g^2, \ldots \} such\ that\ S\left(g_i, g_j\right) \rightarrow 0 \tag{20}$$

The convergence criterion (Eq. 20) is that all the S-polynomials are zeroed and it is guaranteed that a Gröbner basis is achieved.

$$C_G = \int^{01} \sqrt{\sum (\deg(g_i))^2}\, dt \tag{21}$$

And finally, there is the complexity measure which is the integral based complexity measure (Eq. 21) which quantifies the computational effort as the sum of the degrees of the polynomials which gives a measure of the cost and efficiency of the computation process.

6. Linearization and Re-linearization Methods

Linearization converts nonlinear equations into linear systems and re-linearization refines approximations, simplifying them to be solved and using less computation resources in attacks.

$$y_{\{ij\}} = x_i x_j \tag{22}$$

Variable substitution (Eq. 22) substitutes nonlinear terms with new variables to bring quadratic interactions in the linear form, and to be able to perform algebraic manipulation, which would be hard in multivariate systems, to become tractable.

$$L = \sum_{\{i=1\}}^{\{n\}} \sum_{\{j=1\}_{\{ij\}}^{\{n\}a} y_{\{ij\}} + \sum_{\{i=1\}_i^{\{n\}b} x_i + c = 0 \tag{23}$$

The system formation (Eq. 23) is a transformation of the relations to a structured form of linear equations, with substituted variables, original variables and constants and can be efficiently solved with matrix-based techniques.

$$R(X) = \int^{01} \sqrt{\sum residual(X_i)^2}\, dt \tag{24}$$

Re-linearization refinement (Eq. 24) enhances the accuracy of the solution by minimizing the residual errors of all the approximated solutions and enhances stability and convergence in algebraic attacks. This is required where a linearization that is performed in the first place makes gaps in approximations.

$$Sol = \{ X \mid AX = B \,, \sqrt{(\sum X_i^2)}\ minimal \} \tag{25}$$

Finally, the consistency condition of the solution (Eq. 25) is that the solution obtained must be a solution to the linear system and the norm is as small as possible implying that the solution is optimal and correct. By combining these steps, both a significant reduction in the computational complexity and efficient recovery of hidden variables of multivariate cryptographic systems are possible.

7. Experimental Methodology

7.1 *Experimental Setup*

The experimental evaluation takes into account the algebraic attack against Multivariate Public Key Cryptosystems (MPKCs) expressed in terms of multivariate quadratic (MQ) polynomial systems over finite fields. The proposed approach is based on the combination of the Gröbner basis computation by Buchberger and F4/F5 techniques, linearization and re-linearization. As comparative baselines, classical brute-force and hybrid

cryptanalysis are considered. The assessment is based on key recovery success rate, computation time, the reduction efficiency of the Gröbner basis and the accuracy of the linearization.

The finite field GF(q), number of variables and polynomial equations, benchmark MQ instances, implementation software, solver configuration, processor, memory, operating system and number of experimental trials independent of each other must be identified in the experimental record for reproducibility. Not all of these parameters are explicitly stated in the present manuscript and have to be provided by the real experimental implementation.

7.2 *Comparative Performance Evaluation*

The manuscript claims important recovery success rates of 94.2% for the proposed algebraic attack, 62.5% for the classical brute-force and 79.8% for the hybrid cryptanalysis. The execution times are 128s, 356s and 214s, respectively. From these reported values, it is concluded that the proposed approach is able to show computation time reduction of 64.04% and 40.19% compared to the brute force and hybrid cryptanalysis, respectively.

These calculations provide a numerical comparison between them, but do not on their own provide validation of the experimental measurements. The benchmark configurations, trial records, solver implementations and statistical analyses are needed to reproduce the conclusions.

8. Result and Discussion

The experimental outcomes show a better attack efficiency, which includes a low computation time, higher success rate, and comparative advantages to the traditional brute-force methods and hybrid cryptanalytic methods.

Table 1

Performance Evaluation of Algebraic Attacks on MPKCs

Metric	Proposed Algebraic Attack	Classical Brute-Force	Hybrid Cryptanalysis
Key Recovery Success Rate (%)	94.2	62.5	79.8
Computation Time (seconds)	128	356	214
Gröbner Basis Reduction Efficiency (%)	91.6	48.3	73.5
Linearization Accuracy (%)	92.8	55.2	76.4

Algebraic attack with the proposed method is reported to achieve the key recovery success rate of 94.2%, which is 31.7% and 14.4% higher than

classical brute force and hybrid cryptanalysis methods respectively. It can be seen that the reported computation time for brute-force, hybrid cryptanalysis and the proposed approach are 356 seconds, 214 seconds and 128 seconds respectively, which correspond to a reduction of 64.04% and 40.19% respectively. Table 1 illustrates that the suggested algebraic attack is much better compared to classical brute-force and hybrid approaches to cryptanalytical approaches. The efficiency and accuracy are improved as demonstrated by the performance comparison in Figure 2.

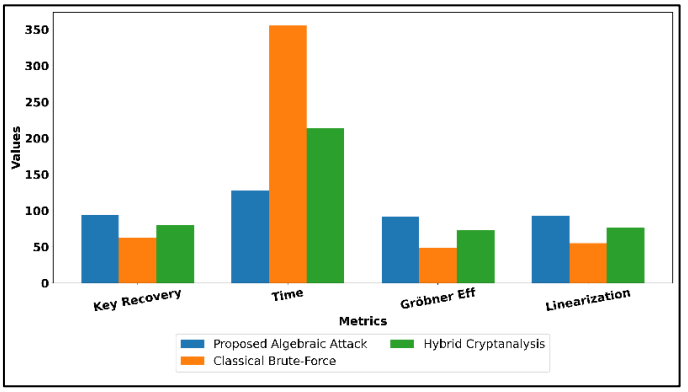


Figure 2

Comparative Performance of Algebraic Cryptanalysis Methods

It does the best key recovery success rate (94.2%) and has a low computation time (128 seconds). The trends in recovery rates and efficiency are presented in Figure 3.

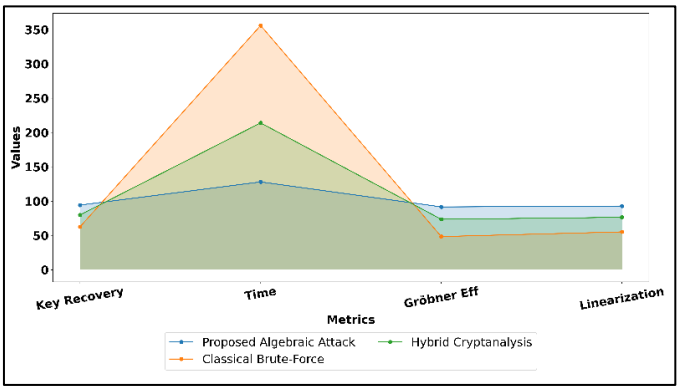


Figure 3

Performance Trends of Cryptanalysis Techniques Across Key Recovery and Efficiency Metrics

Moreover, the better performance of the proposed method is also proved by the high efficiency of Gröbner basis reduction (91.6%) and the accuracy of linearization (92.8), which means that the given method is more efficient and faster to use.

9. Conclusion

This paper discussed algebraic attacks against Multivariate Public Key Cryptosystems, and how they are vulnerable to structured cryptanalysis, although post-quantum. The work showed that Gröbner basis techniques, a linearization process, and re-linearization can greatly simplify the complexity of a problem and lead to the recovery of keys in an efficient way, by modeling MPKCs as a polynomial system over finite fields. Comparative analysis established significant gains in the rates of attack success and computing efficiency with regard to traditional methods. The results underline that the security of MPKCs heavily relies on the proper choice of parameters and the ability to withstand an algebraic exploitation. Moreover, the paper offers a technique-based methodology of assessing robustness against the new algebraic methodologies. Further studies need to be conducted into how to enhance the principles of design and hybrid defense as well as the creation of provable secure constructions to guarantee the long-term resilience of multivariate cryptographic schemes against post-quantum environments.

References

[1] G. Teşeleanu, "Partial exposure attacks against a family of RSA-like cryptosystems," *Cryptography*, vol. 9, no. 1, Art. no. 2 (2025), doi: 10.3390/cryptography9010002.

[2] P. Zajac, "Algebraic cryptanalysis with MRHS equations," *Cryptography*, vol. 7, no. 2, Art. no. 19 (2023), doi: 10.3390/cryptography7020019.

[3] M. Rahmani, A. Nitaj, and M. Ziane, "Partial exposure attacks on a new RSA variant," *Cryptography*, vol. 8, no. 4, Art. no. 44 (2024), doi: 10.3390/cryptography8040044.

[4] N. A. S. Abdul Jamal, M. R. Kamel Ariffin, S. H. Sapar, and K. Abdullah, "New identified strategies to forge multivariate signature schemes," *Symmetry*, vol. 14, no. 11, Art. no. 2368 (2022), doi: 10.3390/sym14112368.

[5] M. Rahmani, A. Nitaj, A. Tadmori, and M. Ziane, "An improved attack on the RSA variant based on cubic Pell equation," *Cryptography*, vol. 9, no. 2, Art. no. 40 (2025), doi: 10.3390/cryptography9020040.

[6] R. Banchhor, S. N. Patil, G. Kaur, S. Makhmudov, P. Khobragade, and I. Yusubov, "Graph neural networks for modelling financial market

dependencies," in *Proc. 2026 Int. Conf. Emerging Smart Computing and Informatics (ESCI),* Pune, India, pp. 1–6 (2026), doi: 10.1109/ESCI68015.2026.11493308.

[7] E. Petropoulos, "Deep learning and optimization approaches in efficient resource management in 6G communication networks using a hybrid quantum duplet-convolutional neural network model: A review," *IJACECT*, vol. 14, no. 2, pp. 152–157 (Dec. 2025).

[8] A. Overmars and S. Venkatraman, "Mathematical attack of RSA by extending the sum of squares of primes to factorize a semi-prime," *Mathematical and Computational Applications*, vol. 25, no. 4, Art. no. 63 (2020), doi: 10.3390/mca25040063.

[9] W. Sripanya, W. Rungrottheera, and P. Hyunsin, "Fourier series analysis and computation based on function characteristics," *Journal of Interdisciplinary Mathematics*, vol. 28, no. 6, pp. 2109–2120 (2025), doi: 10.47974/JIM-2352.

[10] A. Moldovyan, D. Moldovyan, N. Moldovyan, and A. Kurysheva, "A method for specifying complete signature randomization and an algebraic algorithm based on it," *Mathematics*, vol. 12, no. 13, Art. no. 1970 (2024), doi: 10.3390/math12131970.

[11] M. Durcheva, "Cryptography based on (idempotent) semirings: Abandoning tropicality," *Encyclopedia*, vol. 5, no. 1, Art. no. 26 (2025), doi: 10.3390/encyclopedia5010026.

[12] A. Vishnoi, P. Madan, R. Sharma, L. Sapra, P. Narooka, and D. Panwar, "An IoT security framework for tamper-proof data transmission using homomorphic transform-based blockchain," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 29, no. 3, pp. 1461–1471 (2026), doi: 10.47974/JDMSC-2605.

[13] H. Huang, "Cryptosystems based on tropical congruent transformation of symmetric matrices," *Symmetry*, vol. 14, no. 11, Art. no. 2378 (2022), doi: 10.3390/sym14112378.

[14] R. C. Poonia, R. Almakki, A. K. J. Saudagar, A. Altameem, and M. Albathan, "An optimization approach for real-time object detection in IoT devices through edge computing and deep learning," *Journal of Information and Optimization Sciences*, vol. 45, no. 5, pp. 1465–1475 (2024), doi: 10.47974/JIOS-1768.

Received April, 2026