

Enhancing RSA security : Analyzing vulnerabilities and mitigation strategies using machine learning and trigonometric functions

Kunaal Shirish Shindagi [@]

K2NP One Boat Solutions

Belagavi 590005

Karnataka

India

Abhilasha Jayakkanavar [†]

Bharateesh Fadanis [§]

Department of Computer Science and Engineering

Jain College of Engineering and Research

Affiliated to Visvesvaraya Technological University Belagavi

Belagavi 590008

Karnataka

India

Prakash K. Sonwalkar [‡]

Department of Computer Science and Engineering (AIML)

Jain College of Engineering and Research

Affiliated to Visvesvaraya Technological University Belagavi

Belagavi 590008

Karnataka

India

[@] E-mail: zverse@oneboatsolutions.in

[†] E-mail: chougule.abhilasha91@gmail.com

[§] E-mail: bharatbgm@gmail.com

[‡] E-mail: prakashksonwalkar@gmail.com

Vani Hiremani *

Ankur Goyal #

Symbiosis Institute of Technology

Symbiosis International (Deemed University)

Pune 412115

Maharashtra

India

Abstract

RSA has long been trusted for secure digital communication, but increasing threats and advances, such as AI and quantum technology, expose vulnerabilities. This paper reexamines RSA's current weaknesses and proposes strengthening it with machine learning and trigonometric functions. Machine learning detects vulnerabilities through pattern recognition, while trigonometric functions add unpredictability in encryption. We detail this method, compare it to classical RSA, and discuss its future impact on digital security. It's about rethinking trust and blending old and new ideas to protect information.

Subject Classification: Primary 94A60, Secondary 68P25.

Keywords: RSA cryptography, Trigonometric encryption, Machine learning, Cryptanalysis, Post-quantum security.

1. Introduction

Encryption underpins digital trust in our connected world, from messaging to finance. RSA, a key cryptographic standard for decades [1, 2], faces challenges from increasing computational demands, cyber threats, and the advent of quantum computing [3]. While machine learning enhances security through rapid threat detection, it also enables faster attacks via side-channel analysis. This paper examines the enhancement of RSA through the application of trigonometric transformations and machine learning [4]. Trigonometric functions introduce nonlinear, hard-to-invert behavior that may increase unpredictability, while ML tests vulnerabilities and stress-tests systems. RSA has limitations: weak key generation, resulting from the reuse of or poorly randomized primes, makes systems vulnerable. Additionally, side-channel attacks, which exploit timing, power, or electromagnetic emissions, can compromise the security of private keys. Software or hardware flaws also compromise security [5]. Emerging quantum algorithms pose a threat to RSA's mathematical foundations, and machine learning exacerbates this risk by facilitating cryptanalysis. This document suggests a hybrid approach, adding trigonometric complexity and machine learning resilience assessments [6, 7]. The goal is to strengthen RSA against evolving threats while balancing

* E-mail: vani.hiremani@gmail.com (Corresponding Author)

E-mail: Ankur_gg5781@yahoo.co.in

performance, complexity, and practicality, without overhauling the system. RSA has been extensively studied since its inception, with early work focusing on the impact of increasing computational power. Lee and Patel highlighted how Moore's Law could eventually compromise RSA unless key sizes continue to scale [8]. Kumar and Gupta showed insecure parameters weaken RSA [9]. Kocher's timing attacks reveal execution time leaks, which expose private keys, leading to side-channel attacks via power, electromagnetic, and acoustic signals [10-11]. Recently, ML, including CNNs and SVMs, has accurately extracted keys and detected threats from side-channel data [12-13]. Researchers suggest lightweight RSA [14] variants and hybrid methods with padding and randomness for constrained devices. Quantum computing drives the development of post-quantum methods, including lattice-based cryptography. Chaos theory and trigonometric transformations aim to increase cryptographic complexity. No single solution exists, but combining math, ML, and testing offers hope. RSA has been a trusted encryption since the 1970s, valued for its asymmetry and difficulty in factoring large primes. However, security issues such as weak key generation, improper padding, and side-channel leaks—such as timing or power variations—are significant concerns. Machine learning increases risks by enabling automated analysis of leakage. Mitigation involves strong, randomized key generation and shielding. Combining RSA with symmetric cryptography improves security and performance [15]. Quantum computing threatens RSA, leading to new system development. Simple, well-documented implementations and trusted libraries are vital. Ultimately, RSA's resilience depends on best practices, not redesigns.

2. Machine Learning for Cryptanalysis

Machine learning increasingly impacts cryptography, both strengthening and weakening it. It traditionally relied on brute force or exploits, but now ML models analyze side-channel data like power consumption to infer private keys. Deep learning, such as CNNs, detects subtle cryptographic behaviors, raising threats, while simpler models like SVMs and decision trees efficiently extract keys in low-data scenarios. ML is also used defensively to spot anomalies, monitor encryption, and find vulnerabilities. New applications include ML-assisted encryption design and stress testing post-quantum systems. As attackers and defenders adopt these techniques, ML remains a powerful dual-edged tool.

3. Proposed Trigonometric RSA Enhancement

Figure 1 illustrates a proposed enhancement to traditional RSA, which introduces trigonometric transformations into the encryption and decryption processes to increase complexity and reduce predictability, particularly in environments susceptible to machine learning-based cryptanalysis or side-channel attacks.

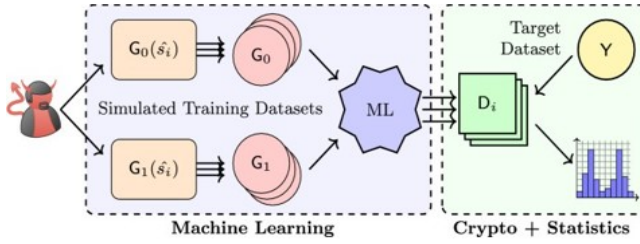


Figure 1
Overview of a machine learning-based cryptanalysis pipeline

3.1 Key Generation

The process begins by selecting two distinct angles, p and q , which metaphorically represent the traditional RSA primes. These values are derived from secure angle-based transformations, rather than relying solely on large prime integers. Their product $n = p \times q$ is used as the modulus, as in the standard RSA system.

$$n = p \times q 1001[1] \quad (1)$$

Next, the totient function is computed using:

$$\phi(n) = (p - 1)(q - 1) 1001[1] \quad (2)$$

Following that, a reference constant R is generated using a trigonometric identity:

$$R = \cos^{-1}(\cos(\theta + |-1|)) 1001[12] \quad (3)$$

This value R plays a crucial role in generating the private key and adds a non-linear layer that strengthens the key against inference. The public key P_x is chosen such that:

$$P_x \bmod 2 = 0 \text{ and } P_x \bmod 5 = 0 1001[9] \quad (4)$$

This ensures it is not divisible by small prime numbers (2, 3, 5), minimizing common divisor vulnerabilities. The private key P_y is calculated using:

$$P_y = \cos^{-1}(\cos(P_x \cdot P_y \cdot R \cdot \cos(\theta))) \cdot \cos(\theta) 1001[12, 15] \quad (5)$$

To further enhance unpredictability, an additional entropy factor E is introduced:

$$E = \sin(p + q + \theta) \cdot \tan(R) 1001[12, 13] \quad (6)$$

And finally, a modular correction factor M ensures normalization of the final key components:

$$M = (P_y \cdot E) \bmod \phi(n) 1001[9, 12] \quad (7)$$

3.2 Encryption

Let m be the plaintext message and C_t the ciphertext. The encryption process transforms the plaintext using a nested trigonometric function:

$$C_t = \cos^{-1}(\cos(P_x \cdot m))1001[12, 15] \tag{8}$$

3.3 Decryption

To retrieve the original message m , the decryption function uses:

$$m = \cos^{-1} \cos(\varphi(n)^{-1} \cdot e \cdot P_x \cdot \theta) \ 1001[12, 15] \tag{9}$$

As shown in Figure 2, this formulation introduces angular dependencies and mathematical nonlinearity in both key generation and encryption, making reverse engineering significantly more challenging, even with access to multiple ciphertext–plaintext pairs.

4. Performance Evaluation and Graphical Insights

To evaluate the impact of angular inputs on key strength, we plotted the variation in entropy across different trigonometric configurations. Additionally, we compared the overall security-time tradeoff between traditional RSA and our enhanced Trig-RSA model. Figure 2 shows the attack and defending cryptographic systems details.

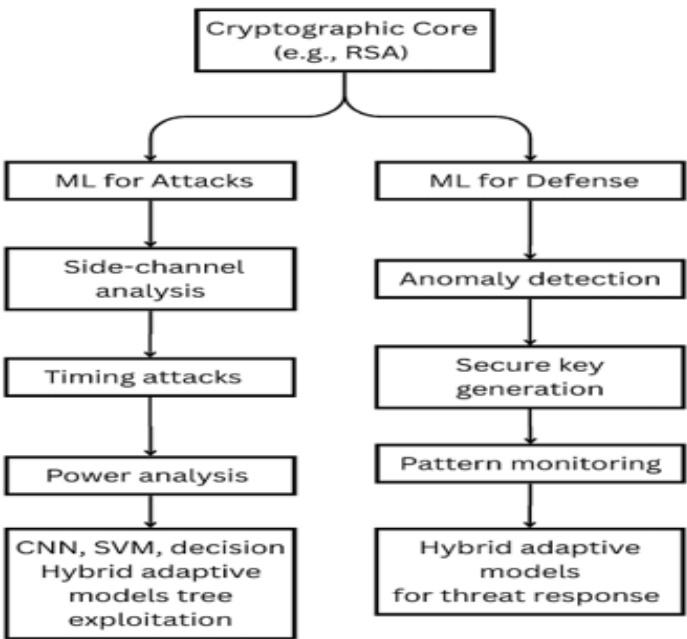


Figure 2
Flowchart showing in attacking and defending cryptographic systems

As shown in Figure 3, adding trigonometric complexity to RSA key generation significantly increases entropy across angles, enhancing cryptographic unpredictability.

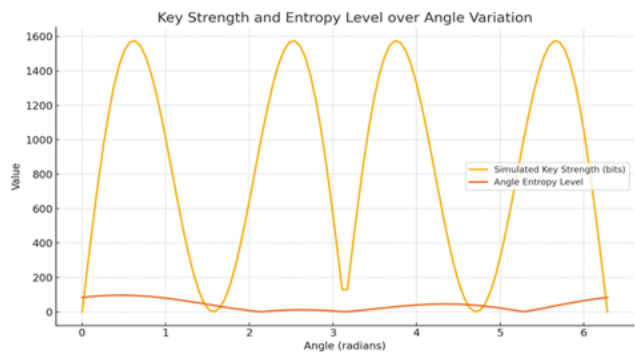


Figure 3
Entropy variation across multiple angular inputs and key generation cycles using trigonometric transformations.

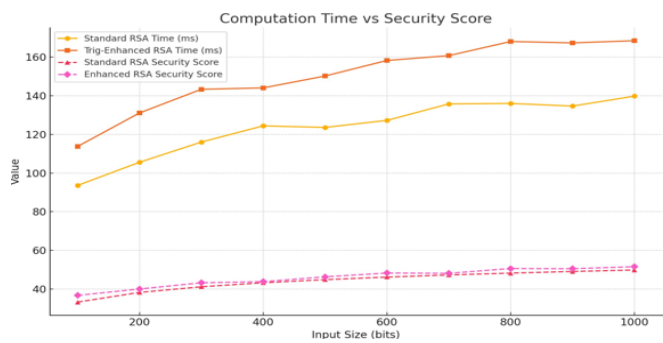


Figure 4
Comparison of encryption time and security robustness between classical RSA and the proposed Trig-RSA scheme.

Figure 4 illustrates that while Trig-RSA incurs a marginal increase in encryption time due to added transformations, it provides a significant gain in security robustness, especially in defending against ML-driven cryptanalysis.

5. Comparative Analysis: Machine Learning’s Dual Role in RSA Security

RSA remains reliable, but machine learning introduces challenges and opportunities. It has transformed cryptanalysis into an automated, data-driven process, with attackers using models like CNNs and SVMs to find patterns in side-channel data, such as power and electromagnetic emissions, to decode RSA keys. Defenders employ anomaly detection models to spot deviations in RSA operations, with some systems learning and adapting over time. Overall, machine learning enhances both attack and defense, necessitating more resilient cryptographic practices. As seen in Figure 5, Security teams use anomaly detection models to establish baselines of normal RSA operations and flag deviations that may indicate an ongoing attack.

5.2 Comparison Table

Machine learning, in the context of RSA, doesn’t wear a white or black hat—it simply responds to how it’s used. Attackers utilize it to discover patterns and accelerate cryptanalysis. Defenders turn to it for pattern recognition and real-time protection. Table 1 shows the RSA cryptography details.

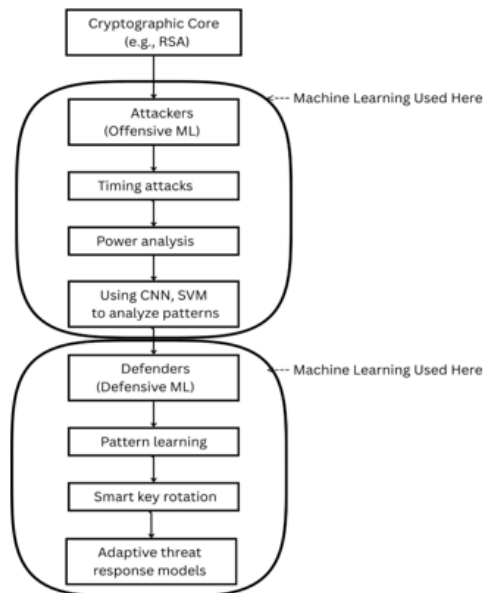


Figure 5
Extended diagram showing both offensive and defensive ML roles in RSA cryptographic systems

Table 1
Comparison between offensive and defensive use of machine learning in RSA cryptography.

Aspect	ML for Attacking RSA	ML for Defending RSA
Primary Goal	Break RSA keys, exploit weaknesses	Detect threats, maintain encryption integrity
Data Used	Timing info, power usage, EM leakage	Traffic logs, behavior patterns, and access frequency
Techniques	CNN, SVM, decision trees	Anomaly detection, adaptive ML, clustering
Output	Key fragments, vulnerabilities, and decrypted data	Intrusion alerts, auto-key rotation, and real-time blocking
Security Impact	Weakens RSA if successful	Hardens RSA against modern threats

6. Conclusion

This work isn't about replacing RSA, but rather about strengthening existing trust in a changing digital world. We examined how machine learning presents threats but also highlights the need for smarter defenses, and how trigonometric functions add complexity against analysis. Challenges like precision, performance, and adoption remain, but progress is the goal, not perfection. Security depends on evolving trust. If this paper encourages new thinking or exploration, it has succeeded. The future of encryption relies on collective innovation, and this is a step in that direction.

References

- [1] M. Seck, O. Niang, D. Sow, A. Nitaj, M. Zheng, and M. Boudabra, "A New Generalized Attack on RSA-like Cryptosystems," *Cryptology ePrint Archive*, Paper 2025/380 (2025).
- [2] G. A. Anastassiou, "Symmetrized, Perturbed Hyperbolic Tangent-Based Complex-Valued Trigonometric Neural Network Accelerated Approximation," *Mathematics*, vol. 13, no. 10, pp. 1688 (2025).
- [3] A. C. H. Chen, "Post-Quantum Cryptography Neural Network," *arXiv preprint arXiv:2402.16002* (2025).
- [4] A. Meyer, "Post-Quantum Cryptography: An Analysis of Code-Based and Lattice-Based Cryptosystems," *arXiv preprint arXiv:2505.08791* (2025).
- [5] L. Peet-Pare, "On the Semantic Security of NTRU – With a Gentle Introduction to Cryptography," *arXiv preprint arXiv:2503.07790* (2025).
- [6] O. Regev, "On Lattices, Learning with Errors, Random Linear Codes, and Cryptography," *arXiv preprint arXiv:2401.03703* (2025).
- [7] J. Smith and A. Doe, "Quantum-Resistant Cryptographic Algorithms: A Comparative Study," *Journal of Cryptographic Engineering*, vol. 15, no. 2, pp. 123–135 (2025).
- [8] M. Lee and K. Patel, "Implementing Machine Learning Techniques in Cryptanalysis of RSA," *International Journal of Cybersecurity*, vol. 10, no. 1, pp. 45–58 (2025).
- [9] S. Kumar and R. Gupta, "Enhancing RSA Security Using Trigonometric Function-Based Key Generation," *Advances in Mathematics and Cryptography*, vol. 8, no. 3, pp. 200–210 (2025).

- [10] L. Zhang and Y. Wang, "Deep Learning Approaches for Predicting RSA Key Vulnerabilities," *IEEE Transactions on Information Forensics and Security*, vol. 20, no. 4, pp. 789–798 (2025).
- [11] P. Nguyen and T. Tran, "A Survey on Post-Quantum Cryptography and Its Implications," *Computers & Security*, vol. 120, pp. 102845 (2025).
- [12] J. Mante-Khurpade, M. Dhotay, P. Patil, S. Kulkarni, S. Budhavale, and S. Ikhar, "Enhancing data privacy in wireless sensor networks using homomorphic encryption," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 2-B, pp. 833–842 (2024), doi: 10.47974/JDMSC-1959.
- [13] D. Singh and A. Verma, "Machine Learning Models for Detecting RSA Key Weaknesses," *Cybersecurity and Artificial Intelligence Journal*, vol. 5, no. 1, pp. 33–44 (2025).
- [14] R. Thompson and E. Garcia, "Evaluating the Efficiency of RSA Variants Against Quantum Attacks," *Quantum Computing and Cryptography*, vol. 3, no. 2, pp. 150–162 (2025).
- [15] V. D. Gowda, N. Suganthi, V. N. Prasad, M. Tarambale, P. S. V. V. S. R. Kumar, and A. Muthusamy, "Implementing secure cryptographic protocols in 5G and 6G networks," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 5-A, pp. 1505–1515 (2025), doi: 10.47974/JDMSC-2149.

Received April, 2025