Cryptanalysis Challenge Brief: Quantum-Disruptive RSA (QD-RSA)

Kapodistrian Academy of Science

May 12, 2025

Overview

Quantum-Disruptive RSA (QD-RSA) is a modified asymmetric cryptographic framework built on top of classical RSA. It introduces three layered transformations designed to mitigate quantum attacks, including those exploiting Shor's and Grover's algorithms, and attacks from annealer-based optimization machines. This brief invites the global cryptographic research community to critically evaluate, analyze, and challenge the security of QD-RSA through open cryptanalysis.

Target of Evaluation

The QD-RSA system modifies standard RSA encryption via the following three layers:

1. **Session-Masked Oscillatory Encoding:**

$$\Phi_s(x) = x \cdot \sin((\pi + \epsilon_s) \cdot x) \mod n \tag{1}$$

   where ϵ_s is derived via HMAC from a session seed. The function is chaotic and non-periodic modulo n.

2. **Entropy-Shifted Nonconvex Trap Function:**

$$\Xi_s(x) = (x + r)^2 \cdot \cosh(\gamma(x + r)) \cdot \tan^{-1}(\delta(x + r)) \mod n \tag{2}$$

   where r is session-specific. The function creates a non-convex energy surface to resist regression and annealing attacks.

3. **Post-Quantum Integrity Hash:**

$$\mathcal{I}_s^*(x) = \text{SHA3-256}\left(\sum_{k=1}^{N_s} \frac{x^k}{b^k}\right) \tag{3}$$

   with N_s and b drawn from session entropy. This layer is designed to resist Grover-enhanced preimage and collision attacks.

Challenge Objectives

Reviewers and adversarial cryptanalysts are invited to challenge the following assumptions:

- That $\Phi_s(x)$ cannot be inverted or approximated without knowledge of ϵ_s and r.
- That $\Xi_s(x)$ is not amenable to surrogate inversion or symbolic regression under bounded oracle access.
- That $\mathcal{I}_s^*(x)$ is not vulnerable to collision or preimage attacks within practical Grover bounds.

Public Parameters

- $n = pq$ where p, q are 1024-bit primes.
- $e = 65537$, $d = e^{-1} \mod \varphi(n)$.
- Fixed values for demonstration: $\gamma = 1.3$, $\delta = 0.8$, $b = 10$, $N_s = 20$.
- Sample entropy strings, ciphertexts, and hashes provided via GitHub repository: `https://github.com/Galactic-Code-Developers/QD-RSA-Challenge`

Submission Guidelines

Submissions may include:

- Full or partial inverse algorithms against any transformation layer.
- Reduced-complexity approximations or exploitable shortcuts.
- Side-channel vulnerabilities or symbolic leakage attacks.
- Grover-adapted quantum search paths through the hash.

All findings will be credited and published under open peer-review. Successful cryptanalysis will contribute to formalizing or revising QD-RSA parameters.

Contact and Disclosure

All challenge submissions should be sent to:

- `validation@kapodistrian.edu.gr`
- Subject: `[QD-RSA Challenge Submission]`

Submissions should include full methodology, tools used, and mathematical basis. Contributors retain credit and may co-author follow-up analysis.