

# QD-RSA Cryptographic Version Declaration

Kapodistrian Academy of Science

May 12, 2025

## Cryptosystem Identifier

- **Name:** Quantum-Disruptive RSA (QD-RSA)
- **Version:** v1.2
- **Date of Publication:** May 12, 2025
- **Maintainer:** Kapodistrian Academy of Science
- **Contact:** validation@kapodistrian.edu.gr

## Version Summary

Version **v1.2** of QD-RSA introduces security-hardened symbolic layers atop classical RSA to resist quantum computational attacks. It addresses previously identified vulnerabilities in the original draft version (v1.0) by incorporating the following improvements:

1.  $\Phi(x) \rightarrow \Phi_s(x)$ : Session-specific entropy injection using

$$\Phi_s(x) = x \cdot \sin((\pi + \epsilon_s) \cdot x) \mod n \quad (1)$$

where  $\epsilon_s = \text{HMAC}(K, s) \mod 10^{-8}$  prevents precomputed inverse matching and Fourier-based lookup.

2.  $\Xi(x) \rightarrow \Xi_s(x)$ : Entropy-blinded domain shift using

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

where  $r$  is a session-specific offset deterring surrogate inversion and symbolic regression.

3.  $\mathcal{I}_\infty(x) \rightarrow \mathcal{I}_s^*(x)$ : SHA3-256-wrapped symbolic hashing using

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

to resist Grover-amplified hash collisions and preimages.

## Backdoor-Free Guarantee

QD-RSA v1.2 is designed and published under a strict zero-backdoor policy. There is no mechanism—cryptographic or procedural—by which any agency, system, or government entity can decrypt QD-RSA-protected messages without possession of both the private RSA key and the session-specific entropy parameters  $(\epsilon_s, r)$ . The protocol includes no escrow key, no master override, no trapdoor, and no embedded bypass channel. This guarantee aligns with the principles of open, post-quantum, trustless cryptography.