NOVAK Cryptographic Challenge v1.0

Purpose:

To evaluate whether the NOVAK Protocol's execution-integrity guarantees can be violated without detection.

Success Categories:

A: Undetected Input Manipulation

B: Undetected Rule Manipulation

C: Undetected Output Manipulation

D: Broken Safety Gate

E: RGAC Chain Break

F: Execution Without Proof

Adversary Models:

- Dolev–Yao++

- Internal adversary

- AI/automation adversary

- Human PS-X adversary

- Physical PL-X adversary

- Regulatory adversary

Submission Requirements:

1. Adversary model used

2. Attack steps

3. Environment details

4. HVET/EIR/RGAC observations

5. Safety Gate behavior

6. Violated NOVAK laws

7. Minimal working proof

Status:

Version 1.0 — Challenge Open

Citation:

Novak, Matthew. The NOVAK Cryptographic Challenge v1.0. NOVAK Protocol Standards Series. 2025.