ZK Proctor

UNIVERSITY OF TARTU
Institute of Computer Science

Prove you didn't cheat — without revealing what you did

PROBLEM

Traditional online proctoring records screens, webcams, and microphones. For 100 candidates: ~500 GB storage, ~200 hours of manual review, zero privacy

THE SOLUTION

A lightweight local agent monitors system activity during an exam, then generates a ZK-STARK proof (~300 KB) that the candidate followed the rules. The verifier checks the proof in ~3 ms without ever seeing what the candidate actually did.

SYSTEM PIPELINE

STARK/FRI implemented in Wolfram Mathematica (zero external libraries).

Config (JSON) → OS Agent + Browser Extension → Execution trace → STARK prover → Verifier

ARITHMETIZATION

All arithmetic in prime field F_p - $p = 2^{61} - 1$ (Mersenne prime) - Inversion: $a^{-1} = a^{p-2} \bmod p$

Trace columns:

$comp[i] \in \{0, 1\}$ — compliant or violation

$vc[i] \in [0, N]$ — violation count

Interpolation via NTT:

$\omega = g^{((p-1)/N)} \bmod p$

$comp(\omega^i) = comp[i]$ for $i = 0,\ldots,N-1$

AIR Constraint Polynomial:

$$C(x) = comp(x)\cdot(comp(x) - 1) + comp(x)\cdot(vc(x) - vc(x\cdot\omega^{-1}))$$

$C(x) = 0 \ \forall x \in D \Rightarrow$ session valid

Soundness: $\varepsilon = 2^{-16}$ with 16 FRI queries

FRI PROVER

FRI Folding — Round k:

1. Commit $f_k \rightarrow$ Merkle root r_k
2. $\alpha_k \leftarrow$ Fiat-Shamir$(r_0 \| \ldots \| r_k)$
3. $f_k(x) = f_{even}(x^2) + x\cdot f_{odd}(x^2)$
4. $f_{(k+1)}(x) = f_{even}(x) + \alpha_k\cdot f_{odd}(x)$
5. deg halves each round
6. Repeat until $|D| \le 4$

FRI VERIFIER

Per-query verification (each layer k):

1. Read $f_k(\omega^i)$ and sibling $f_k(-\omega^i)$
2. Verify Merkle paths against root r_k
3. Recompute α_k from transcript
4. Check folding: computed = committed
5. Final layer: f_L must be constant

Total: $3\times16\times7\times2 = 672$ hash checks

Completed in ~3 ms

USE CASES

Technical Hiring - **University Exams** - **Online Competitions**

https://github.com/sofiascalzo/UniTartu-Contest-ZK-proctor | Sofia Scalzo | Bachelor's level | Computer Science | Contest UniTartu 2026