

# atoi Proof of Correctness Report – Team 2

Matthew Sheldon, Isabella Pereira, Jarrod Rogers, Naja-Lee Habboush, and Brandon Wang

The University of Texas at Dallas,

{mts200002,iap200002,jtr190004,nih200000,blw190004}@utdallas.edu

**Abstract**—TODO.

**Index Terms**—Language-Based Security, Proof of Correctness,  
TODO

## I. INTRODUCTION

**T**ODO (TODO)

## II. MOTIVATION

TODO

## III. PROBLEM DEFINITION

TODO

### A. Primal Point Generation

TODO

### B. Dual Point Generation

TODO

### C. Verification Algorithm Variant

TODO

### D. Quadratic Residue Distribution

TODO

## IV. SUBTRACTIVE QUADRATIC RESIDUE SAMPLING

TODO

## V. COMPARATIVE PERFORMANCE

TODO

### A. Algorithm Throughput

TODO

### B. Algorithm “Uniform Randomness”

TODO

1) Chi-Squared Test: TODO

2) COV Measure: TODO

3) Mesh Ratio: TODO

## VI. FUTURE WORK

TODO

## VII. CONCLUSION

TODO