

# atoi Proof of Correctness Report – Team 2

## Matthew Sheldon

matthew.sheldon@utdallas.edu  
The University of Texas at Dallas  
Richardson, Texas, USA

## Isabella Pereira

isabella.pereira@utdallas.edu  
The University of Texas at Dallas  
Richardson, Texas, USA

## Jarrold Rogers

jarrod.rogers@utdallas.edu  
The University of Texas at Dallas  
Richardson, Texas, USA

## Naja-Lee Habboush

naja-lee.babboush@utdallas.edu  
The University of Texas at Dallas  
Richardson, Texas, USA

## Brandon Wang

brandon.wang@utdallas.edu  
The University of Texas at Dallas  
Richardson, Texas, USA

*Abstract*—**TODO.**

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

2) *COV Measure*: TODO

3) *Mesh Ratio*: TODO

VI. FUTURE WORK

I. INTRODUCTION

TODO

**T**ODO (TODO)

II. MOTIVATION

TODO

TODO

VII. CONCLUSION

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 Througput*

TODO

B. *Algorithm “Uniform Randomness”*

TODO

1) *Chi-Squared Test*: TODO