MARVIN JONES

+1(864) 293-0479 ⋄ Williamston, SC
jonesmc8@gmail.com ⋄ LinkedIn

OBJECTIVE

Cryptography Researcher with 8 months of industry experience and 3+ years of experience in academia researching interactive protocols, verifiable computing and zero-knowledge arguments, seeking full-time employment.

EDUCATION

Ph.D. in Mathematical Sciences, Clemson University — Expected 2023
Field: Zero-Knowledge Proofs
Advisor: Shuhong Gao

- Self-contained introduction of zero-knowledge arguments/proofs to zk-SNARKs for a mathematical audience. Include full detail of constructions and proofs for major techniques and protocols. Additionally, cover known issues in implementations (such as Frozen Heart and Infinite Inflation Glitch).
- Fill in literature gaps for applying various techniques to other protocols. Such as aggregating proofs of Pinocchio and Sonic using techniques snarkpack. This includes implementations in Rust benchmarks and complexity tables for general analysis.
- Provide formalization to arguments that implicitly use reductions (IP that maps relations to a different relation). Additionally, provide results known for IP's for reductions such as AND and OR.
- Protocols for finite precision arithmetic.
- Construct, prove and implement a variety of protocols for matrix multiplication with generalized splitting and folding for matrices.
- Currently, developing a new zk-SNARK that uses Plonk's arithmetic circuit.
- Construct and analyze specialize circuit gates that handle quadratic equations with respect to two variables. This would be between a variety of arithmetic circuits and QAP/R1CS.

M.S. in Mathematics, University of South Carolina — 2014
Thesis title: *On the Group of Transvections of ADE-Diagrams.*
Advisor: Jesse Kass

M.A. in Mathematics, Wake Forest University — 2012
Thesis title: *Solutions of the cubic Fermat equation in quadratic fields.*
Advisor: Jeremy Rouse

B.S. in Mathematics, Winthrop University — 2010
Minor: Computer Science

EXPERIENCE

Cryptography Researcher May 2022 - Dec 2022
Space and Time

- Researched and Designed protocols for Proof of SQL.
- Implemented protocols in Rust for Proof of Concept.
- Wrote a blog post explaining some underlying cryptographic primitives.

Assistant Professor Sept 2016 - Aug 2018
Greenville Technical College *Greenville, SC*

- Created and maintained Webassign homeworks and Blackboard shells for courses I was lead instructor for.
- Created diagnostics to determine readiness of students entering College Algebra.
- Taught a variety of math courses in both university transfer track (College Algebra through Calculus 3) and terminal math courses for associates degrees.
- Tutored students in the math center.

Instructor Aug 2014 - Sept 2016
Greenville Technical College *Greenville, SC*

PROJECTS

Proof of SQL. Researched and designed protocols to verifiably prove the validity of SQL queries based on database commitments. Investigated design choices to improve overall complexities of the scheme. Implemented protocols during proof of concept phase in Rust.

PUBLICATIONS

- Jessica Bennett, Shuhong Gao, Hunter Handley, M. Jones, Aram Lindroth, Yu-Chung Liu, Emily Sundberg, Kyle Yates, 'Novel Matrix Multiplication Interactive Protocol by Split-and-Folding Reductions,' *In Preparation.*
- M. Jones, Linds Wise, 'Spherical Visual Cryptography,' *In Preparation.*
- M. Jones, Jeremy Rouse, 'Solutions of the cubic Fermat equation in quadratic fields,' *International Journal of Number Theory.* **9**, no. 6, (2013), 1579-1591.

SKILLS

Programming Languages: C++/C, Java, Processing, Rust, Solidity