Report on *The BSS model and cryptography*, Kristina Hostáková

The Blum-Shub-Smale (BSS) model of computation, as studied in this thesis, essentially consists of a machine with a finite number of registers, which can each store a single real number. The machine can do arithmetic operations $+, -, \cdot, \div$ and also exact comparisons $=, <, \leq$ in unit time, and some of the registers can start out containing built-in constants.

This thesis sets out to study functions which are easy to compute and hard to invert in this model. "Easy to compute" generally means constant time, and the "hard to invert" question turns into looking at time bounds on approximating roots of rational functions. In particular the main result of the thesis is a lower bound of $\Omega(\log(\log(N) - \log(\epsilon)))$ elementary computation steps to approximate $\sqrt{x}$ on the interval $[0, N]$, on a machine with no built-in constants other than 0 or 1. The thesis also contains careful, detailed presentations of upper bounds on the square root and the general problem of inverting a BSS machine.

I am not qualified to say how new the main result is; a cursory search doesn't show anything. I did not find any problems worth noting in the proofs, although I have not gone through all the details. The presentation of the thesis is excellent. Everything is done with great care and at an appropriately high level of rigour, while remaining clear and a pleasure to read. I am impressed by the mathematical maturity displayed in this work. I strongly recommend that the candidate successfully defends it.

Neil Thapen 1 June 2016