

Real numbers are usually represented by various discrete objects such as floating points or partial decimal expansions. This is mainly because the classical computability theory relates to computers which work with discrete data. Nevertheless, for theoretical purposes it is interesting to look at models of computation that deal with real numbers as with objects of unit size. A very natural such model was suggested by Blum, Shub and Smale in 1989.

In 2012 Grigoriev and Nikolenko studied various cryptographic tasks involving real numbers (for example, biometric authentication) and they considered the BSS machine model. In this work we focus on hard to invert functions in this model of computation. Our main theme is to analyse whether there are real functions of one variable that are easier to compute than to invert by a BSS machine.