

Reálná čísla jsou obvykle reprezentována různými diskrétními objekty, například plovoucí řádovou čárkou nebo částečným desetinným rozvojem. A to zejména proto, že se klasická teorie vyčíslitelnosti váže k počítačům, které pracují s diskrétními daty. Nicméně z teoretického hlediska je zajímavé uvažovat i výpočetní modely, které pracují s reálnými čísly jako s objekty velikosti jedna. Blum, Shub a Smale v roce 1989 takový model navrhli.

V roce 2012 se Grigoriev a Nikolenko zabývali různými kryptografickými úlohami, které se přirozeně týkají reálných čísel (například biometrickou autentizací) a uvažovali při tom výpočetní model BSS. V této práci se zaměřujeme na těžko invertovatelné funkce v tomto výpočetním modelu. Naším hlavním cílem je zkoumat, zda existují reálné funkce jedné proměnné, které se BSS strojem snáze počítají než invertují.