

Tato práce se zabývá dávkovými důkazy pro mocnění (dávky PoE). Zkoumáme existující dávkové PoE a analyzujeme jejich ověřovací náklady. Také představujeme dva dávkové PoE a porovnáváme jejich výkon s výkonem existujících přístupů. Naše dávkové PoE překonávají existující, jak teoreticky, tak i prakticky. Zlepšení ověřovacích nákladů dosahujeme snížením očekávaného počtu grupových násobení. Pro praktickou analýzu vybíráme hodnoty parametrů protokolu používané v praxi a pak měříme čas násobení a mocnění na straně ověřovatele pro zkoumané protokoly v naší implementaci v jazyce C++.