Lucasovy posloupnosti jsou konstantní rekurzivní celočíselné posloupnosti s dlouhou historií aplikací v kryptografii - používané jak pro návrh kryptografických schémat, tak při kryptoanalýze. V této práci představujeme ověřitelné zpožďovací funkce založené na sekvenční náročnosti výpočtu Lucasových posloupností v RSA grupě.

Zaprvé ukážeme, že modulární Lucasovy poslopnosti jsou alespoň tak sekvenční, jako jsou klasické zpožďovací funkce založené na iterovaném modulárním mocnění představené Rivestem, Shamirem, and Wagnerem v kontextu tzv. time-lock puzzles. Navíc nenacházíme žádnou očividnou opačnou redukci, což nás přivádí k domněnce, že počítání modulárních Lucasových poslopností je ostře složitější než modulární iterované mocnění. Jinými slovy, námi kostruovaná zpoždovací funkce si zachová svoji sekvenčnost i v případě nalezení nového efektivnějšího algoritmu pro modulární iterováné mocnění.

Zadruhé představíme praktickou konstrukci ověřitelné zpožďovací funkce založené na modulárních Lucasových posloupnostech. Naše konstrukce vychází z nedávné práce Pietrzaka (ITCS 2019) a využívá souvislost mezi problémem výpočtu modulárních Lucasových posloupností a mocněním v příslušném tělesovém rozšíření.