Lucas sequences are constant-recursive integer sequences with a long history of applications in cryptography, both in the design of cryptographic schemes and cryptanalysis. In this work, we study the sequential hardness of computing Lucas sequences over an RSA modulus.

First, we show that modular Lucas sequences are at least as sequentially hard as the classical delay function given by iterated modular squaring proposed by Rivest, Shamir, and Wagner in the context of time-lock puzzles. Moreover, there is no obvious reduction in the other direction, which suggests that the assumption of sequential hardness of modular Lucas sequences is strictly weaker than that of iterated modular squaring. In other words, the sequential hardness of modular Lucas sequences might hold even in the case of an algorithmic improvement violating the sequential hardness of iterated modular squaring.

Second, we demonstrate the feasibility of constructing practically efficient *verifiable* delay functions based on the sequential hardness of modular Lucas sequences. Our construction builds on the work of Pietrzak (ITCS 2019) by leveraging the intrinsic connection between the problem of computing modular Lucas sequences and exponentiation in an appropriate extension field.