601.645 Practical Cryptographic Systems
Final Project Draft **Sunitha Narayan**

Construct a Verifiable delay function (VDF) to show a way to publicly verify Rivest-Shamir-Wagner time-lock puzzle.

Implementation Details

(a) **Setting**: we require that N = p · q is the product of safe primes (a prime p is safe if $(p-1)/2$ is also prime)

(b) **The Protocol**: The protocol includes a prover, P and a verifier, V where P convinces V that it has solved the RSW puzzle, this is done as follows:

- The verifier V and prover P have as common input an RSW puzzle (N, x, T) and a statistical security parameter λ. Here T $\in \mathbb{N}$, N = p . q is the product of safe primes.
- P solves the puzzle by computing y and sends it to V
- Now, P and V have common input of (N, x, T, y) and the output is either of the form (N, x' , [T /2], y'), in which case it is used as input to the next iteration
- If T = 1 then V outputs accept and reject otherwise.
- The protocol stops with verifier output in either reject, accept

(c) Construct a VDF from RSW

References

(a) Verifiable Delay Functions. Boneh, 2018 [Link]

(b) Efficient verifiable delay functions. Wesolowski, 2018 [Link]

(c) Simple Verifiable Delay Functions. Pietrzak, 2018 [Link]

(d) Time-lock puzzles and timed-release Crypto, [Link]