Project Proposal

Cunningham Chain generator

By: Piriya Hall,Blake Vermeer,Rohit Zambre

Motivation

- Why are prime numbers important?
  - Prime numbers are vital in the field of cryptography.
  - It is very computationally intensive to verify that large numbers are prime. This property is useful as a proof of work in cryptocurrencies.

Motivation

- Cryptographic currency
  - Primecoin
    - Proof-of-work of Primecoin is the generation of prime numbers, specifically Cunningham chains of the first kind, Cunningham chains of the second kind, or Bi-twin chains.

Cunningham Chain of the First Kind

- Cunningham Chain of the first kind is a sequence of prime numbers that follows the pattern $p_{i+1} = 2p_i + 1$.
- The chain is said to be complete when the next number in the sequence is not prime.
- Example: **89, 179, 359, 719, 1439, 2879** (The next number would be 5759 = 13*443, but that is not prime.)

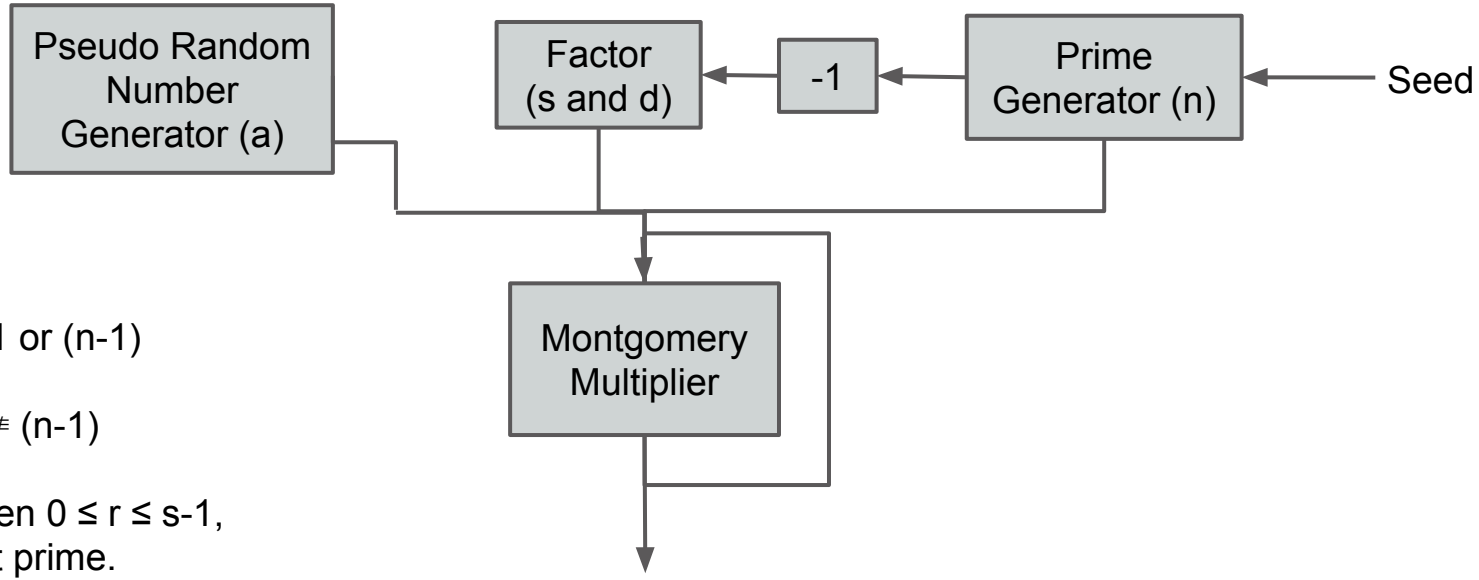
Project Overview

- We plan to implement a Cunningham Chain generator
- Steps needed to generate a Cunningham Chain
  - Generate a prime number
  - Generate the next number in the Cunningham Chain
  - Validate that the number is prime

Final Product

Final product of this project would be a logical circuit on an FPGA that can generate a Cunningham chain of the first kind with x length in a reasonable amount of time.

System Design



Test:

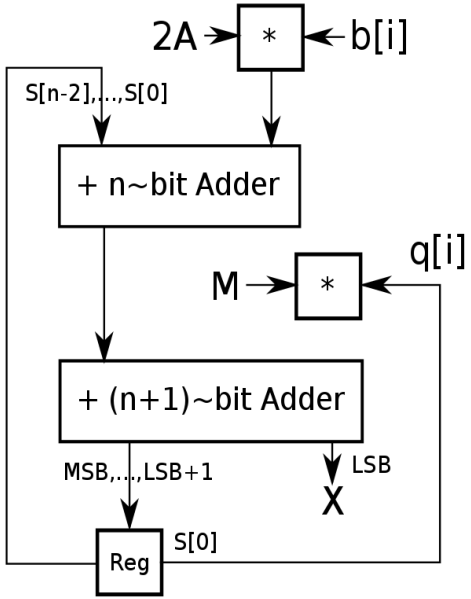
$a^d \bmod n \not\equiv 1$ or $(n-1)$
and
$a^{2rd} \bmod n \not\equiv (n-1)$

for any r when $0 \leq r \leq s-1$,
then n is not prime.

(a = random number < n)
$(n-1 = 2^s d)$

System Design

Montgomery Multiplier



Project Plan

Week 0.5 [Nov 5 - Nov 8]	Get the framework from MP-3 set up for the project
Week 1 [Nov 9 - Nov 15]	Successful Generation of Cunningham Chain number candidates; calculation of s and d.
Week 1.5-2 [Nov 16 - Nov 21]	Start implementation of Montgomery Multiplier; Pseudo-random number generator integrated correctly
Week 2.5 [Dec 1 - Dec 7]	finish implementation of Montgomery Multiplier
Week 3 [Dec 8 - Dec 16]	Attempt to accelerate Montgomery Multiplier and/or factor s and d calculation

Grading Rubric

Attributes	Proficiency/Performance Scale		
	1: Beginning - Unsatisfactory	**2: Accomplished - Satisfactory**	**3: Exemplary - Beyond Satisfactory**
Generate Prime Candidates and Factor (n-1)	Prime candidates or factoring is not reliably [25 points]	Prime numbers are generated and factoring works correctly [50 points]	Prime number generated and factoring is pipelined in design [75 points]
Pseudo Random Number Generator	Unreliable generation of random numbers [25 points]	Random numbers are generated reliably [50 points]	Random number generation is pipelined in design [75 points]
Validate Primes	Montgomery multiplier is implemented by the control logic isn't correct [25 points]	Montgomery multiplier is implemented and control logic is correct [50 points]	Montgomery multiplier is pipelined [75 points]
Demo and report	Limited demo and report [25 points]	Full demo, report includes descriptions of major components [50 points]	Entertaining demo, report includes detailed figures and evaluation results [75 points]

Questions?

Thank you!