OBJECTIVE

• Implement the RSA cryptology algorithm in Bluespec on the XUPV5 FPGA

• 1024-bit keys for higher security
• Meet 50 MHz timing and beat RaspberryPi performance
RSA ENCRYPTION AND DECRYPTION IN HARDWARE

• Benefits
  • Allow device manufacturers to skip inclusion of processors in devices that only require RSA
  • Improved performance, power usage, space

• Cool Application Example
  • Intelligence agencies' covert listening devices (bugs) with secure communication through RSA
ALGORITHM OVERVIEW

• Components:
  • Public Key (n, e)
  • Private Key (n, d)
  • Plaintext Message (m)
  • Ciphertext (c)

• Encryption
  \[ c \equiv m^e \pmod{n} \]

• Decryption
  \[ m \equiv c^d \pmod{n} \]
IMPLEMENTING

\[ \text{data}^\text{exponent} \pmod{\text{modulus}} \]

- Modular Exponentiation
  - Right to Left binary algorithm
  - Computed using a Modulus Multiplication

- Interleaved Modulus Multiplication
  - Multiplication that interleaves the modulus that requires binary shifts, bitwise operations, and additions
MODULAR EXPONENTIATION

- Performs left-right binary exponentiation
- Uses two modular multipliers
- Takes 1024 steps to complete
INTERLEAVED MODULAR MULTIPLICATION

- Performs $A \times B \mod M$
- Scans through bits of $A$, if $A[i]$ is 1, then adds the value of $B$
  - Then corrects for modular overflow
- Optimized to prevent long comparison chain
ADDER DESIGN EXPLORATION

• Objective: to meet 50 MHz for a 1024-bit add

• Solution:
  • Naïve ripple-carry adder
    • Did not meet timing
  • Carry look-ahead adder
    • Clocked at 83.5 MHz
  • Multi-cycle adder
    • Lower performance than CLA
  • Reduced clock frequency adder
    • Did not meet space constraints
TIMING RESULTS

• Achieved 84.5 MHz for 1024-bit RSA (clocked at 50MHz)
  • Completes operation in ~200ms

• Raspberry Pi (700 MHz ARM11) completes an operation in one minute
  • Significant improvement over embedded processors
CONTRIBUTION

• Exceeds RaspberryPi performance using less power: **1.8 W** consumption
• RaspberryPi utilizes **2 W**
• Parametrizable adder architectures:
  • Carry look ahead, multicycle adder modules