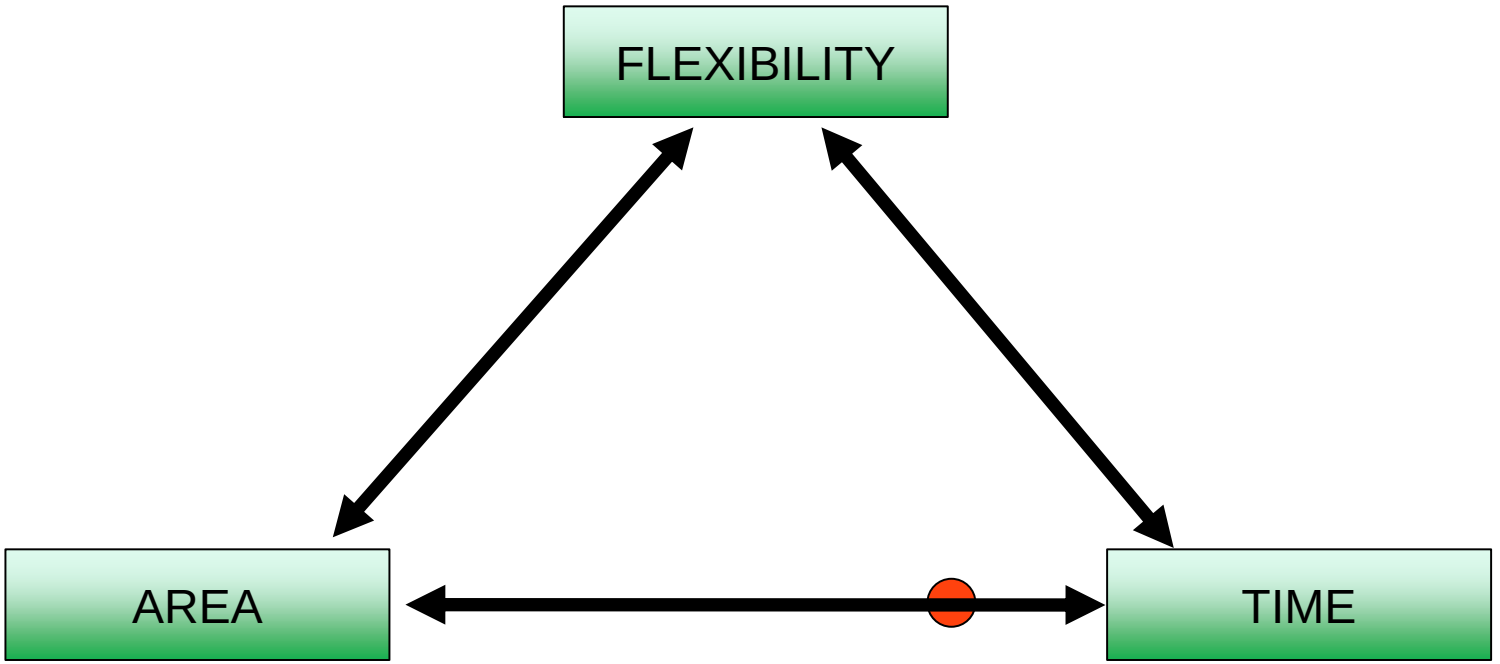
KU LEUVEN

DDP – Final Design

G26 – Yusuf Heylen & Natan Vander Meeren

What did we focus on?

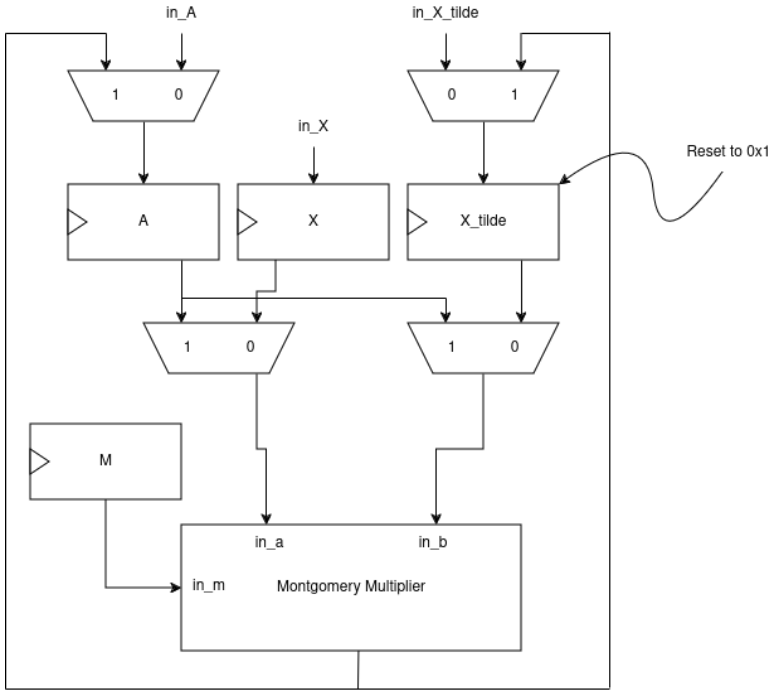


KU LEUVEN

Exponentiation

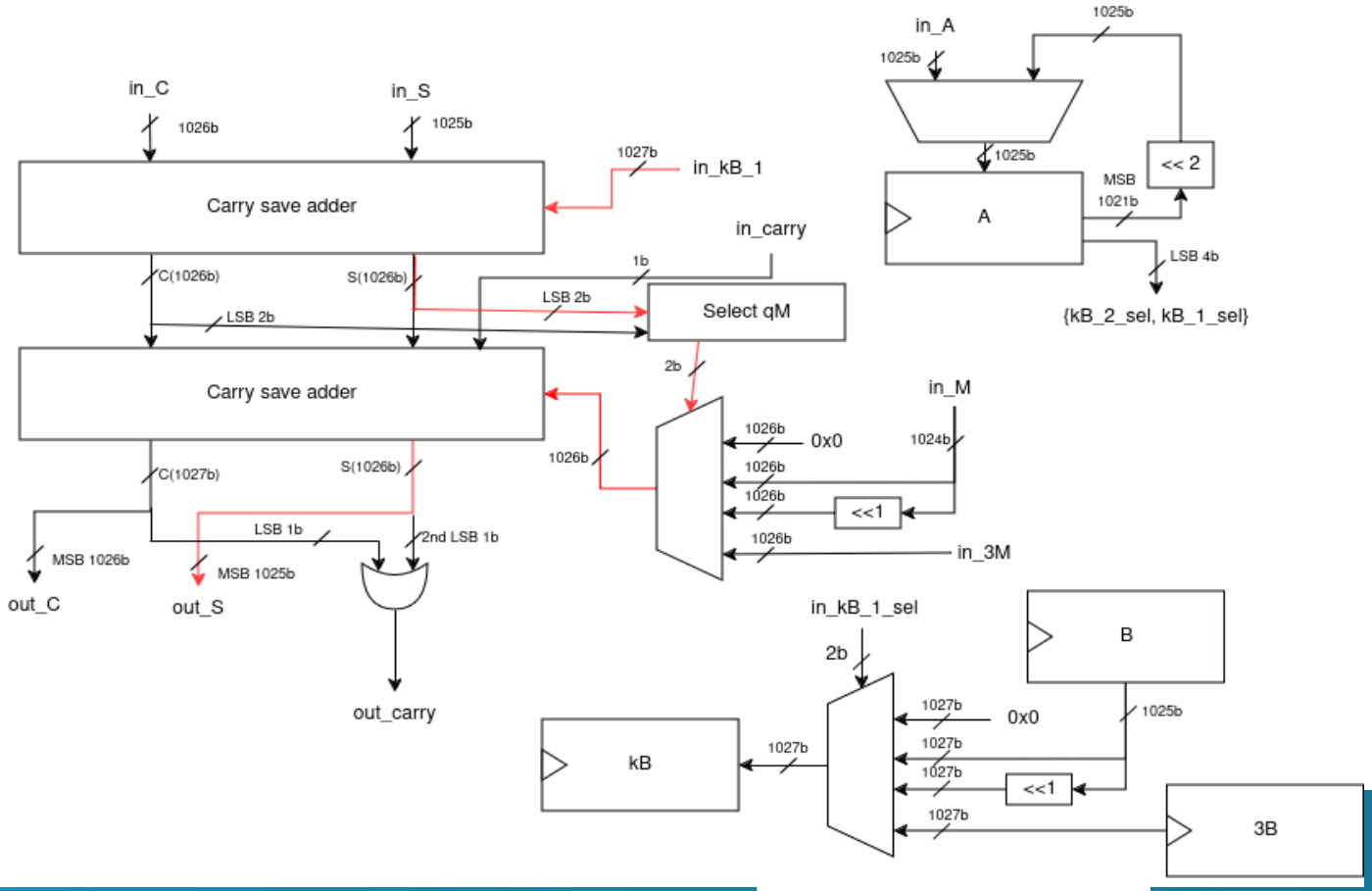
- R → 4R
  - No need for final subcond (but extra MM loop iterations)
- Algorithm modification

  → (1.5e_len+2) montmuls on average
- X resets to 0x1 (saves a MUX)



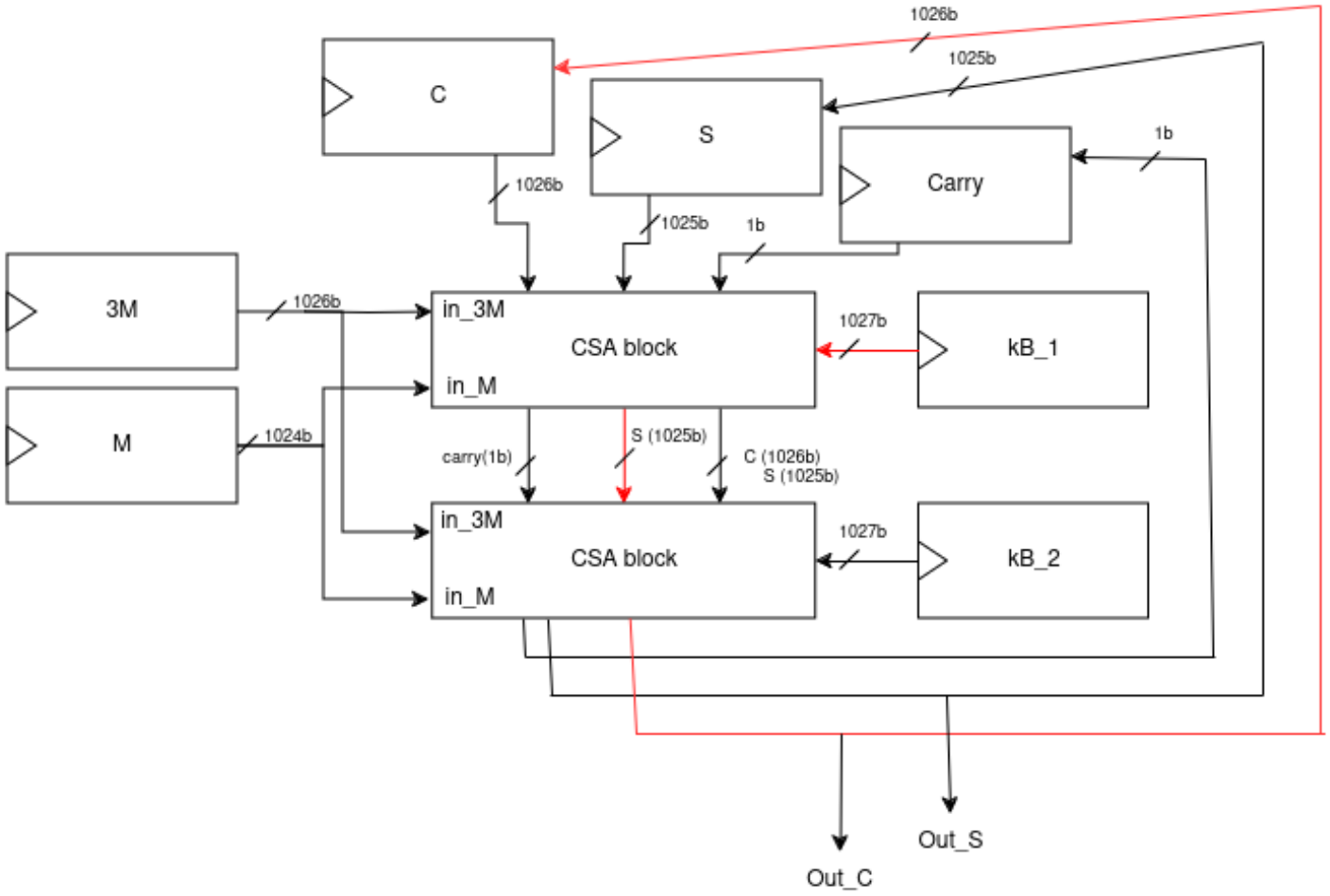
Montgomery multiplication

- Carry-save adder
  - ➔ Idea: X+Y+Z = C+S can be calculated by a row of full adders
  - ➔ Only *real* additions: 3M, 3B, (C+S)



KU LEUVEN

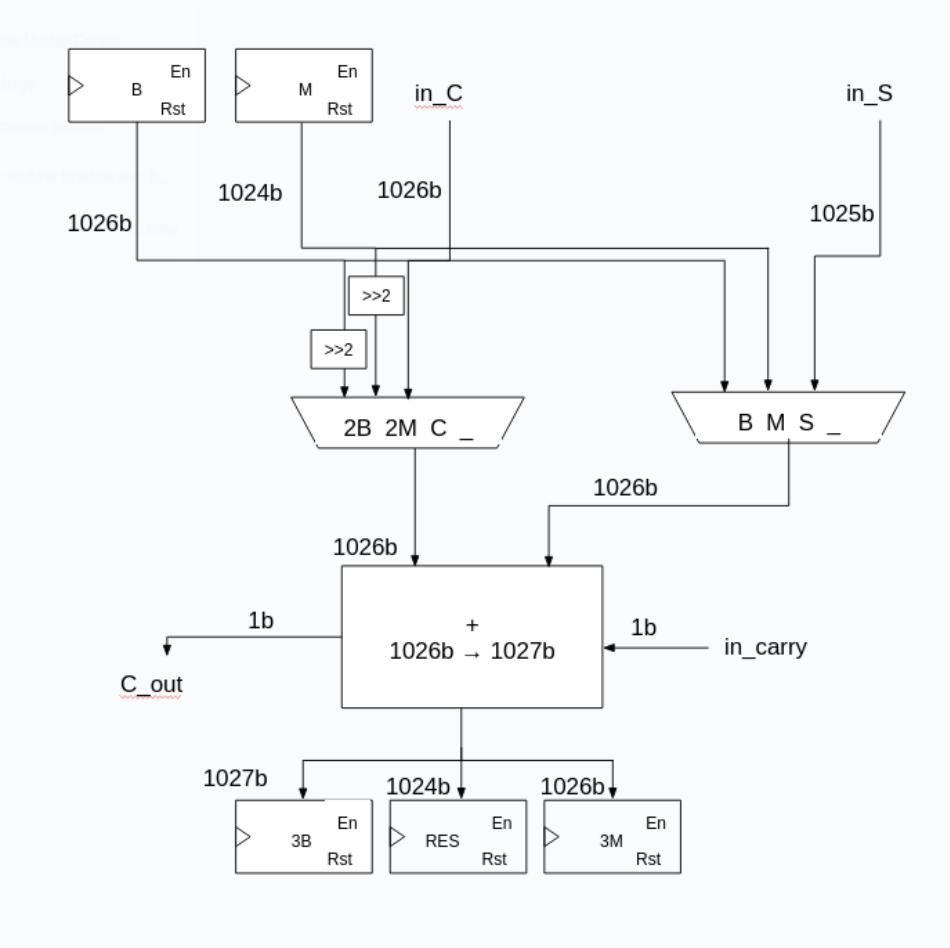
CSA cascade



KU LEUVEN

Adder

- DSP slices
  - Small (22cycles / addition)
    - ➔Easy routing for the other components
    - ➔Allows clock frequency increase (by a lot)



HW/SW interface

- We only used start (0x0) – stop (0x0)
- Exponent length → register
- Large numbers → address in register

Final summary

FFs	LUTs	Clk frequency	SW cycles encryption	SW cycles decryption
27415	19344	125MHz	47381	2662484

- Flexibility?
  - Not the main focus
- Future ideas
  - Booth encoding for higher radix
  - CRT for decryption ➔ /2 speedup

Questions

KU LEUVEN