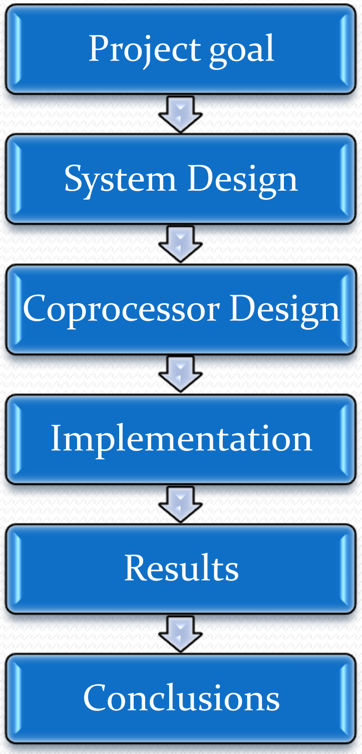
HW/SW Co-design Project

G8:

Boran Car

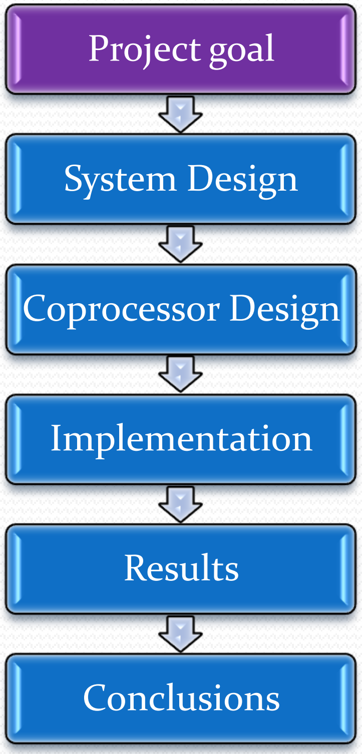
Victor Statescu

Outline



- Project Goal
- System design
- Coprocessor design
- Implementation
- Results
- Conclusions

Project Goal



Project goal

System Design

Coprocessor Design

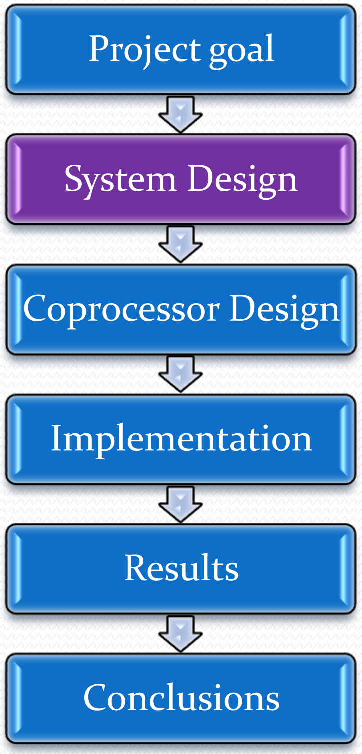
Implementation

Results

Conclusions

- The design of a cryptographic system that would support RSA and ElGamal 1024 bit encryption and decryption

System Components



Project goal

System Design

Coprocessor Design

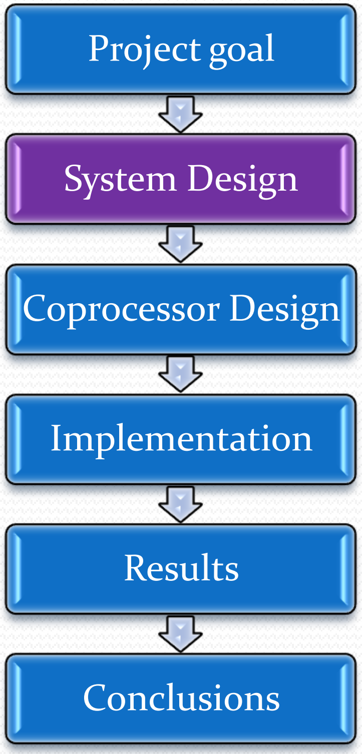
Implementation

Results

Conclusions

- 8051 µController
- Memory mapped interface (shared memory)
  - Possibility of pipeline
  - Limitations of Gezel
- Custom Crypto-Coprocessor

8051 µController


Project goal

System Design

Coprocessor Design

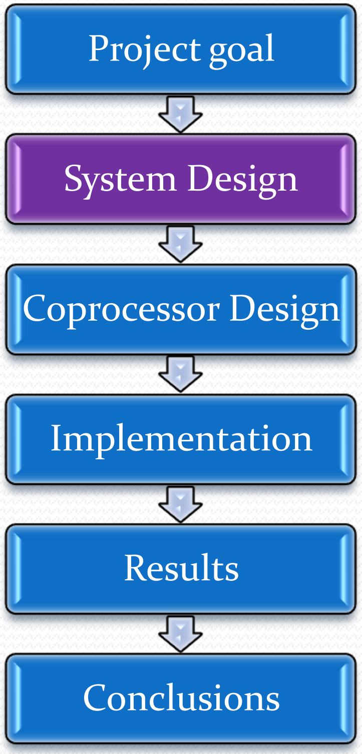
Implementation

Results

Conclusions

- 4 8-bit ports:
  - P1 – used for signaling to the coprocessor;
    - Only two pins used;
  - P0, P2 – used for xbus access;
  - P3 – used for serial I/O, interrupts, control signals, etc.;
- Memory:
  - 2kB + 1 B (512B shared with the coprocessor);

Memory Mapped Interface (shared memory)


Project goal

System Design

Coprocessor Design

Implementation

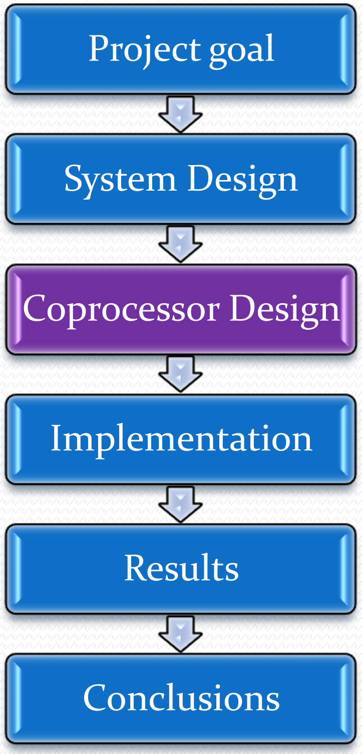
Results

Conclusions

- 512B used to share data with coprocessor;

- Addresses mapping:
  - 0x000 - 0x600 used by the µController;
  - 0x600 – 0x801 mapped into 0x000-0x201 for the coprocessor;

Crypto coprocessor


Project goal

System Design

Coprocessor Design

Implementation

Results

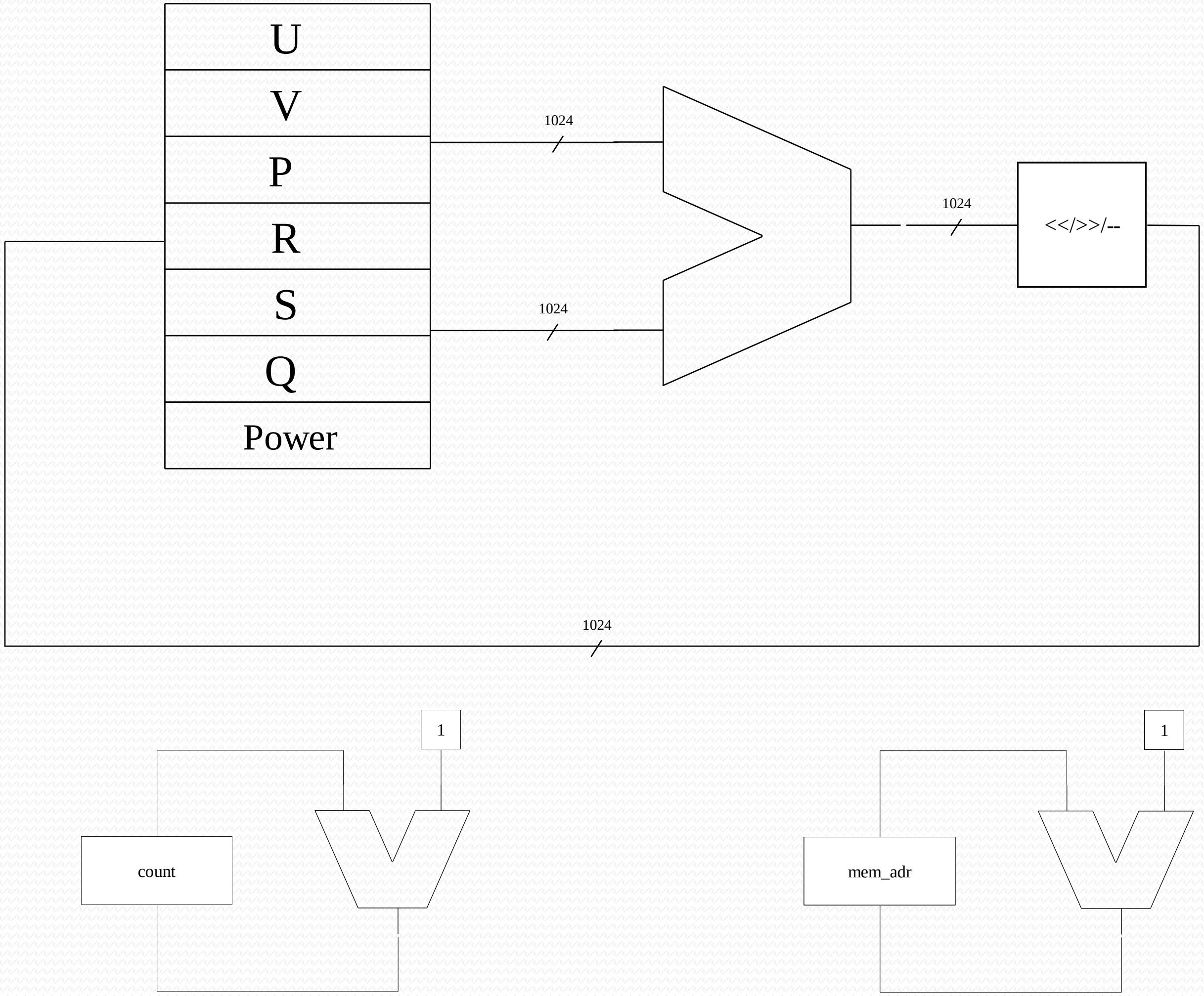
Conclusions

- Operations performed by the dedicated HW:
  - Montgomery product;
  - Montgomery inversion;

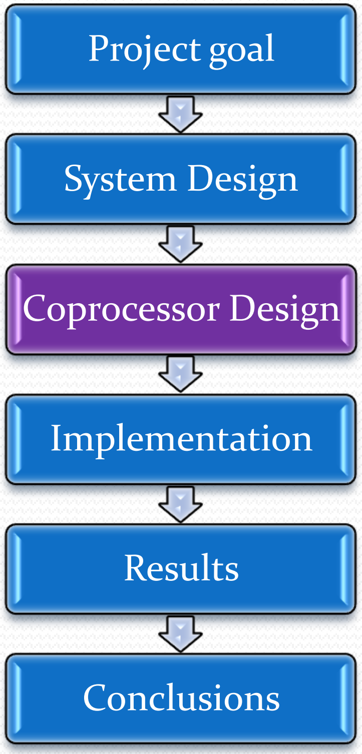
Montgomery multiplication		Montgomery inversion	
SW (12MHz)	HW (12MHz)	SW (12MHz)	HW (12MHz)
1.3 s	0.2 ms	16 s	100 ms

Coprocessor main data-path

- Project goal
- System Design
- Coprocessor Design
- Implementation
- Results
- Conclusions



Memory allocation



Project goal

System Design

Coprocessor Design

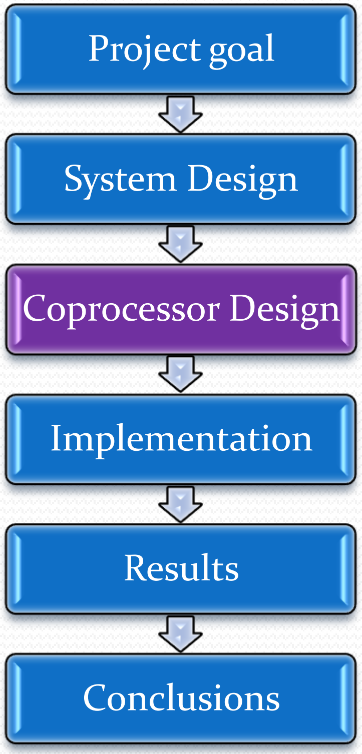
Implementation

Results

Conclusions

- 0x600 - 0x680 1024-bit number;
- 0x680 - 0x700 1024-bit number;
- 0x700 - 0x780 1024-bit number;
- 0x780 - 0x800 command queue (up to 128 commands);
- 0x800 state signaling from the coprocessor;

Instructions implemented


Project goal

System Design

Coprocessor Design

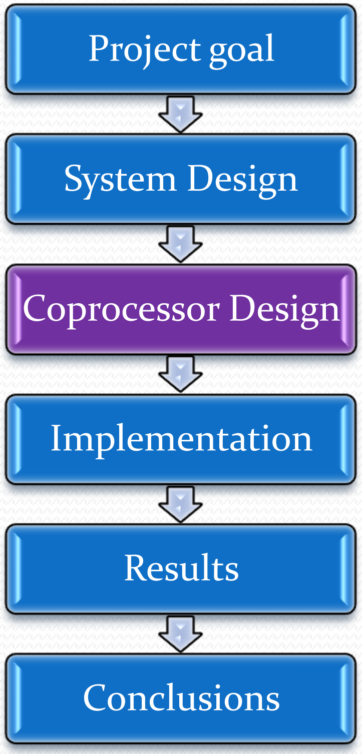
Implementation

Results

Conclusions

- Halt
- Init
- Montgomery multiplication
- Montgomery squaring
- Montgomery inversion
- Load u from the shared memory
- Load v from the shared memory
- Store result to shared memory
- Store quotient to memory (Montgomery only)

Coprocessor improvements



Project goal

System Design

Coprocessor Design

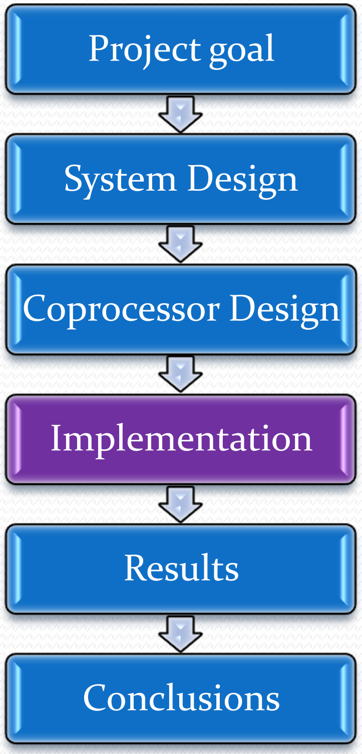
Implementation

Results

Conclusions

- Command queuing:
  - Up to 128 commands can be queued
  - Implemented for:
    - Speed-up;
    - Pipelining;
- Result is written in register u for efficient transitivity;
- Montgomery quotient computation:
  - Doubling the bit-length;

SW implementation



Project goal

System Design

Coprocessor Design

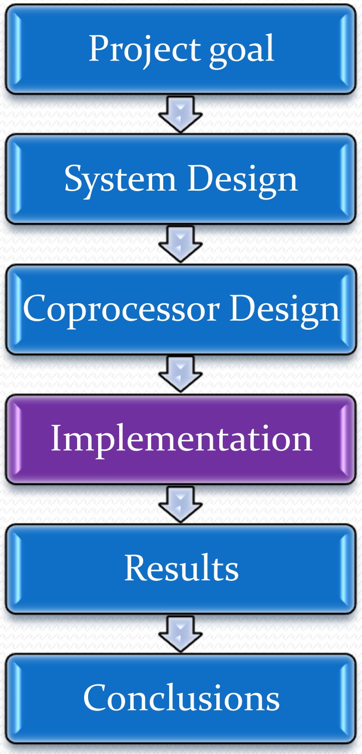
Implementation

Results

Conclusions

- Function library:
  - montpro - Montgomery product
  - montinv - Montgomery inversion
  - modexp - Modular exponentiation
- Methods:
  - add1024 - adding 1024-bit numbers
  - subtract1024 - subtracting 1024-bit numbers
  - multiply1024 - multiplies 1024-bit numbers to produce a 2048-bit
  - larger or equal - checks if the number is larger or equal than a number

HW implementation



Project goal

System Design

Coprocessor Design

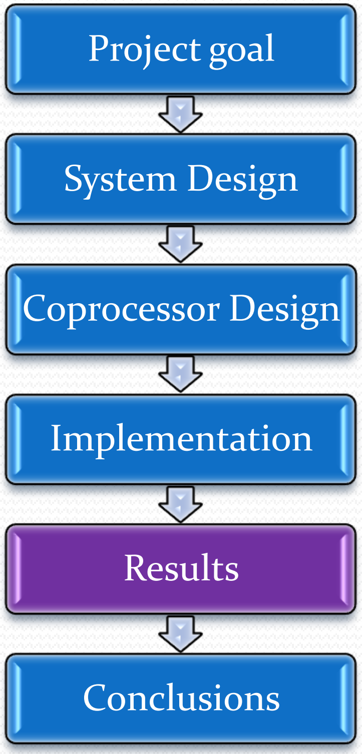
Implementation

Results

Conclusions

- GEZEL to VHDL conversion
- Separate data-paths for adder and shifter:
  - For optimization of critical components
- Manual redesign of the adder (in VHDL);

Results


Project goal

System Design

Coprocessor Design

Implementation

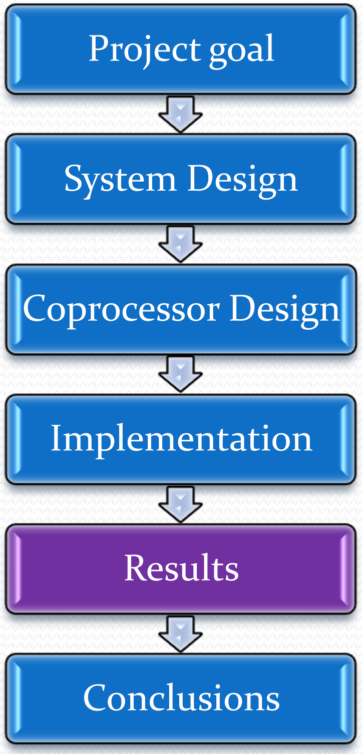
Results

Conclusions

RSA		ElGamal	
# Clock Cycles	Duration	# Clock Cycles	Duration
5 mil	1.25 s	4.5 mil	1.125 s
Frequency = 4MHz			

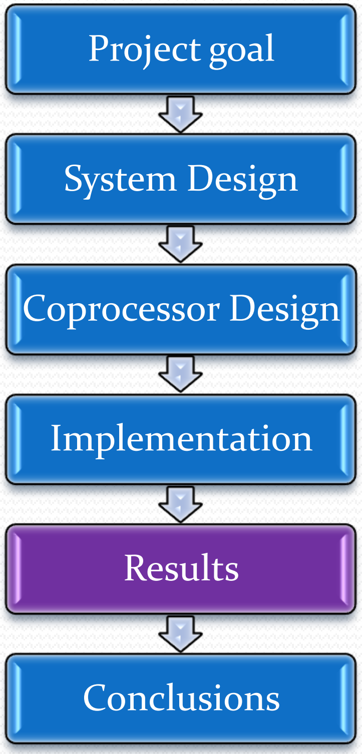
FPGA Results			
	Used	Available	%
Slices	14587	13696	106%
Flip-flops	6274	27392	22%
4-input LUTs	26857	27392	98%

Results



Macro Statistics	
# Adders/Subtractors	4
10-bit adder	2
1026-bit adder carry in	1
11-bit subtractor	1
# Registers	6251
Flip-Flops	6251
# Comparators	1
1024-bit comparator equal	1
# Multiplexers	1
1026-bit 4-to-1 multiplexer	1

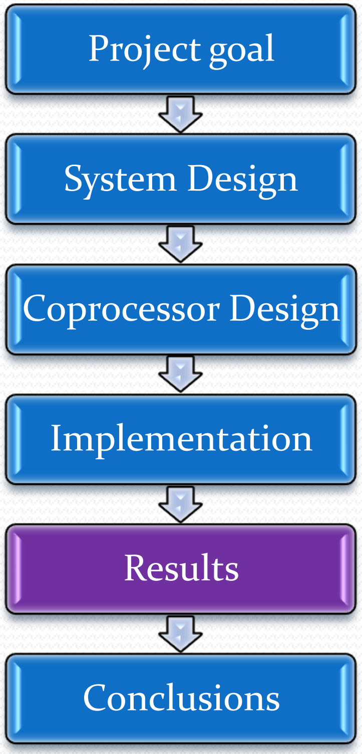
Results



RSA		ElGamal	
# Clock Cycles	Duration	# Clock Cycles	Duration
5 mil	1.25 s	4.5 mil	1.125 s
Frequency = 4MHz			

FPGA Results			
	Used	Available	%
Slices	13951	13696	101%
Flip-flops	6267	27392	22%
4-input LUTs	26033	27392	95%

Results


Project goal

System Design

Coprocessor Design

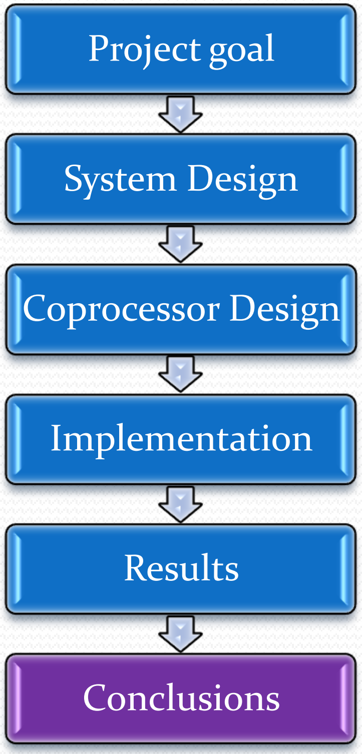
Implementation

Results

Conclusions

Macro Statistics	
# Adders/Subtractors	5
10-bit adder	2
513-bit adder carry in	2
11-bit subtractor	1
# Registers	6251
Flip-Flops	6251
# Comparators	1
1024-bit comparator equal	1
# Multiplexers	1
1026-bit 4-to-1 multiplexer	1

Conclusions



Project goal

System Design

Coprocessor Design

Implementation

Results

Conclusions

- The presented results show that our design is in line with other industrial designs;
- The maximal allowable frequency achieved: 20.449MHz;
- The area requirements were finally met;