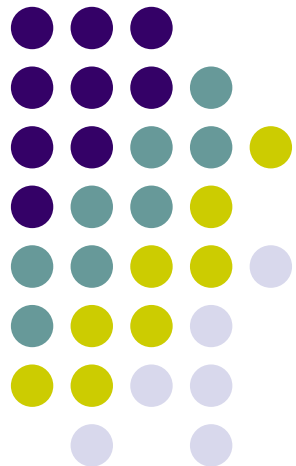
An Implementation Comparison of an IDEA Encryption Cryptosystem on Two General-Purpose Reconfigurable Computers

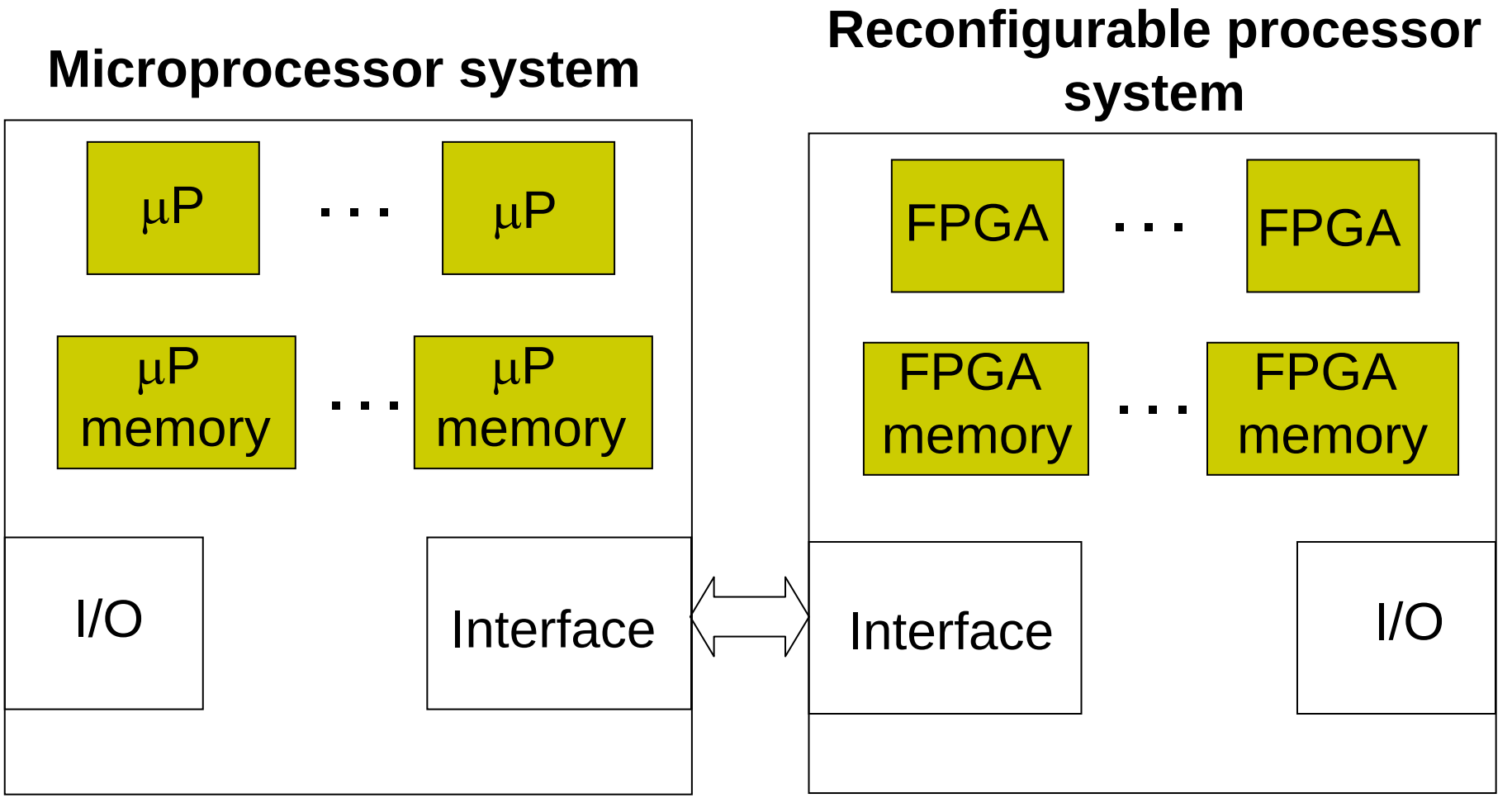
Allen Michalski[1], Kris Gaj[1], Tarek El-Ghazawi[2]

[1] ECE Department, George Mason University

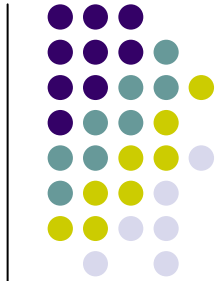
[2] ECE Department, The George Washington University



What is a Reconfigurable Computer?



Characteristic Features

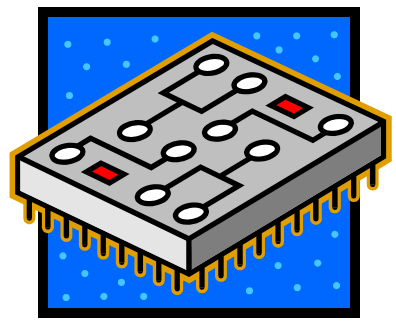


- ✓ composed of traditional microprocessors and FPGAs
- ✓ programming does not require knowledge of hardware design
- ✓ permit run-time reconfiguration of FPGAs

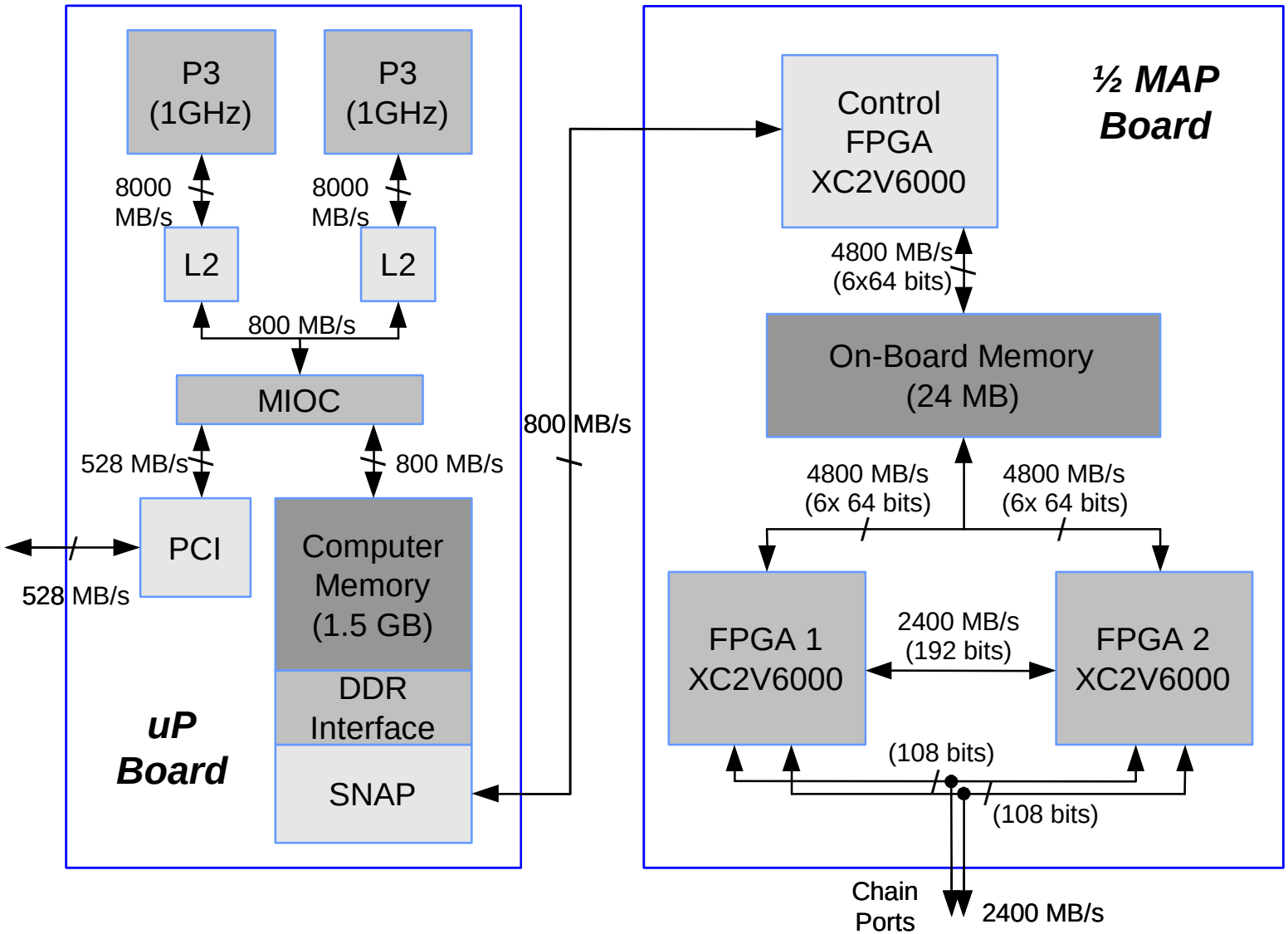
Examples:

- **SRC-6E**
- **Starbridge HC-36**

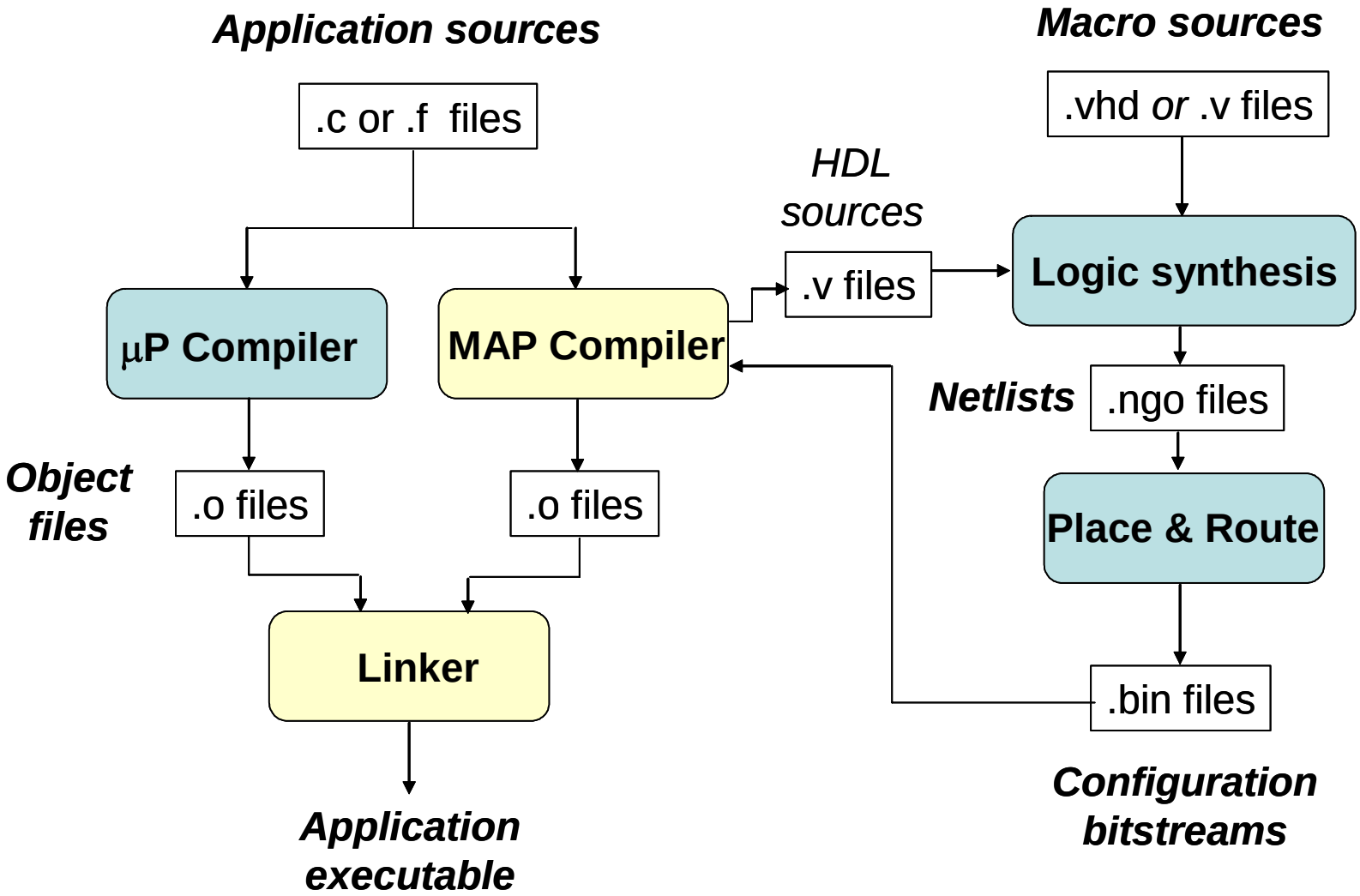
SRC and Star Bridge Systems



SRC Hardware Architecture



SRC Compilation Process



SRC Programming Model

Program in C or Fortran

Main program

……

Function_1(a, d, e)

……

Function_2(d, e, f)

……

Function_1

Macro_1(a, b, c)

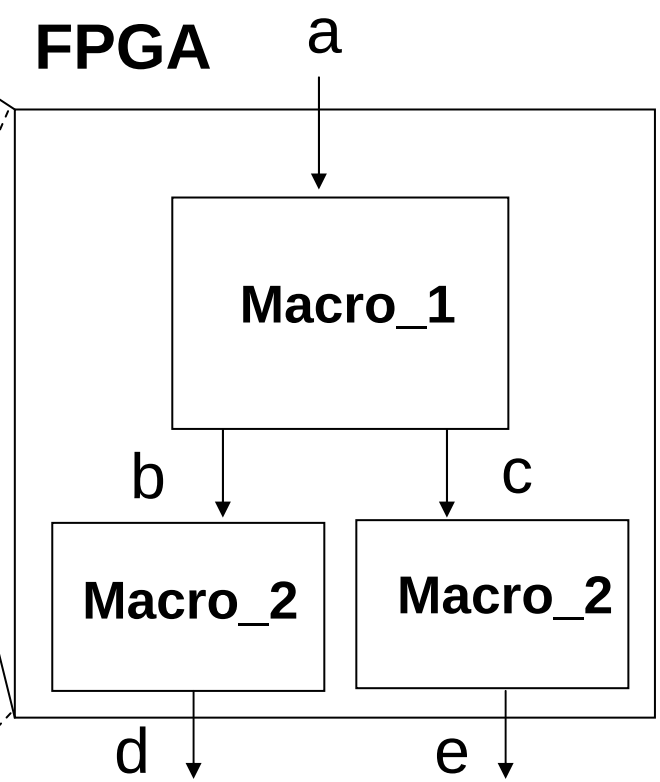
Macro_2(b, d)
Macro_2(c, e)

Function_2

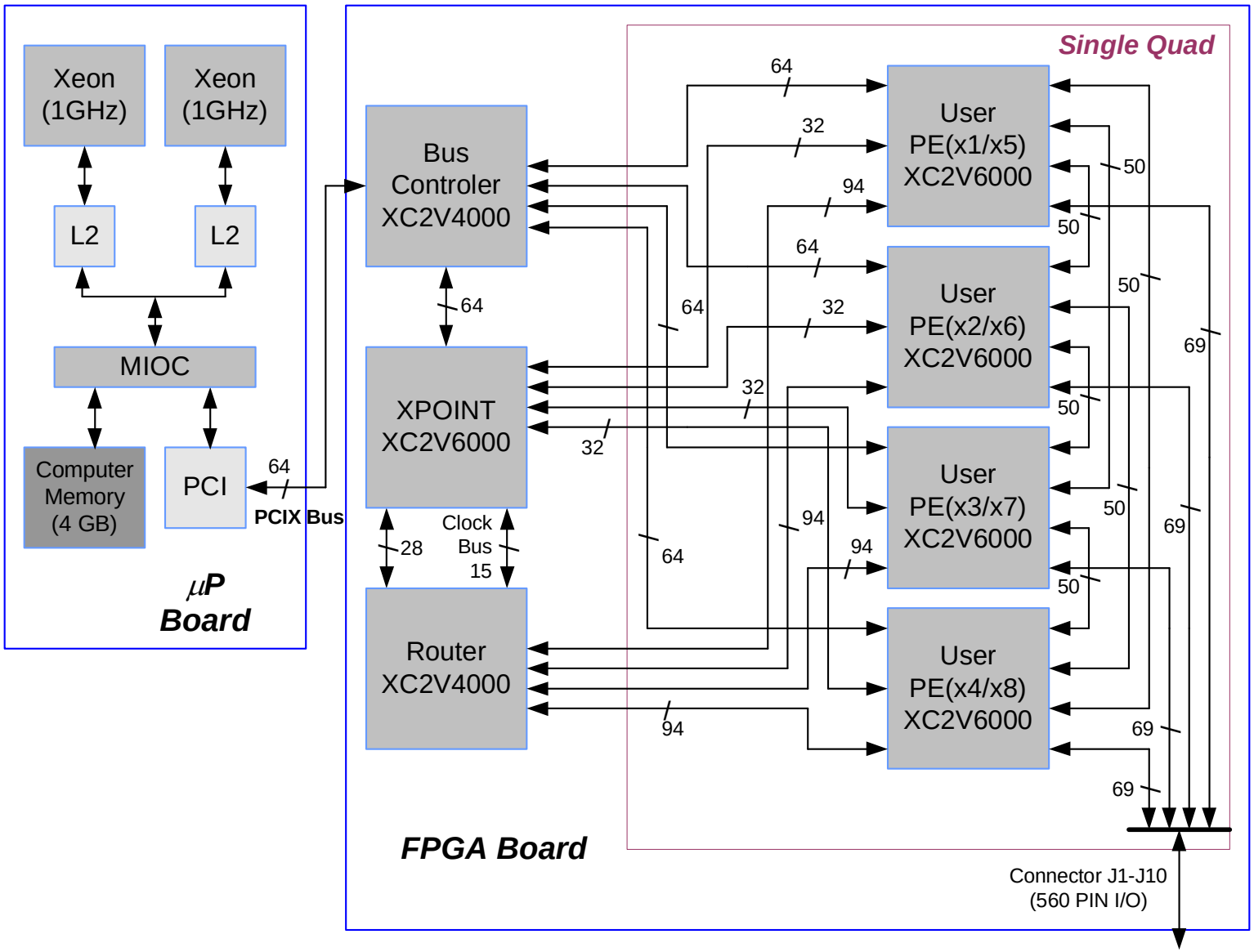
Macro_3(s, t)

Macro_1(n, b)
Macro_4(t, k)

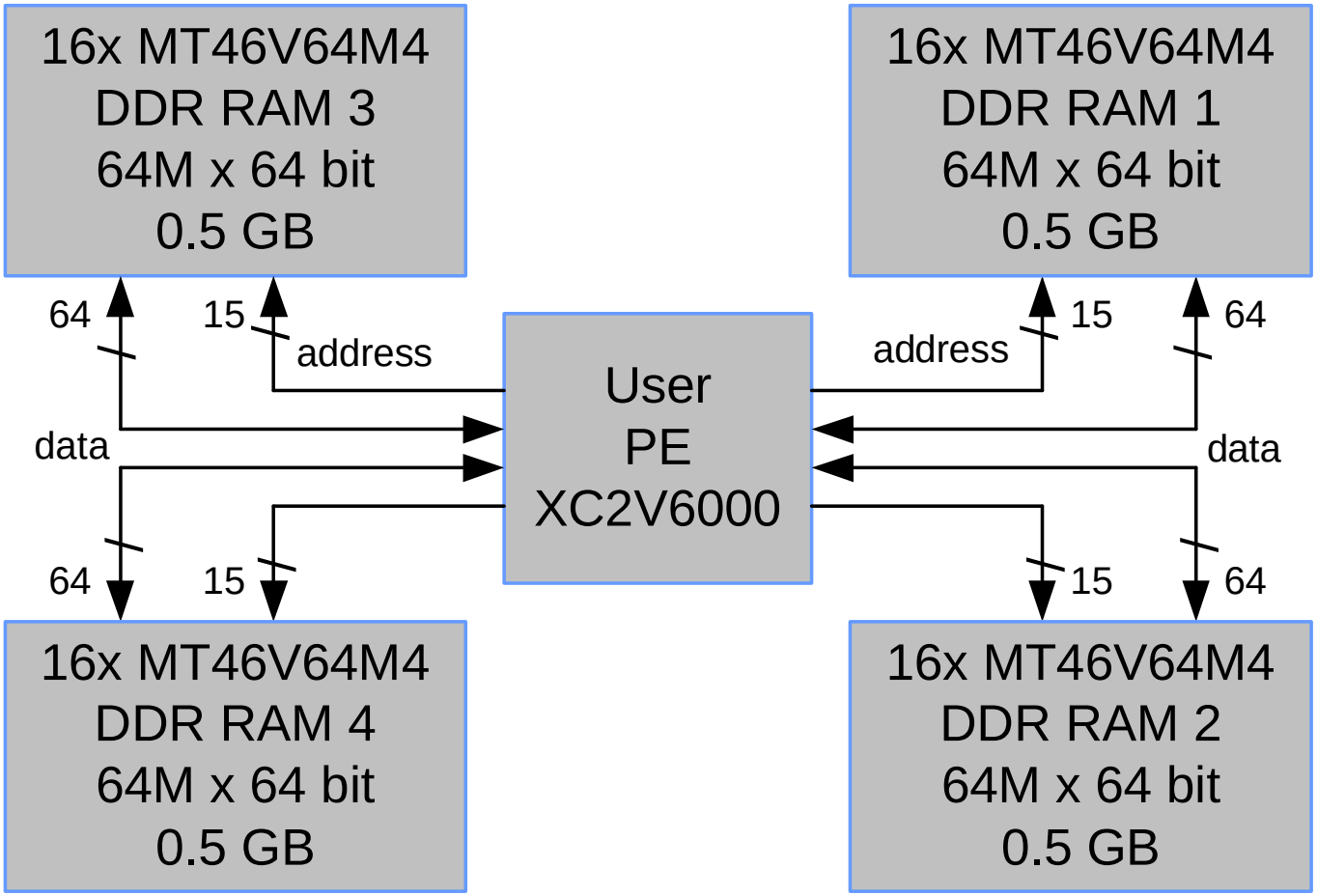
FPGA contents after the Function_1 call

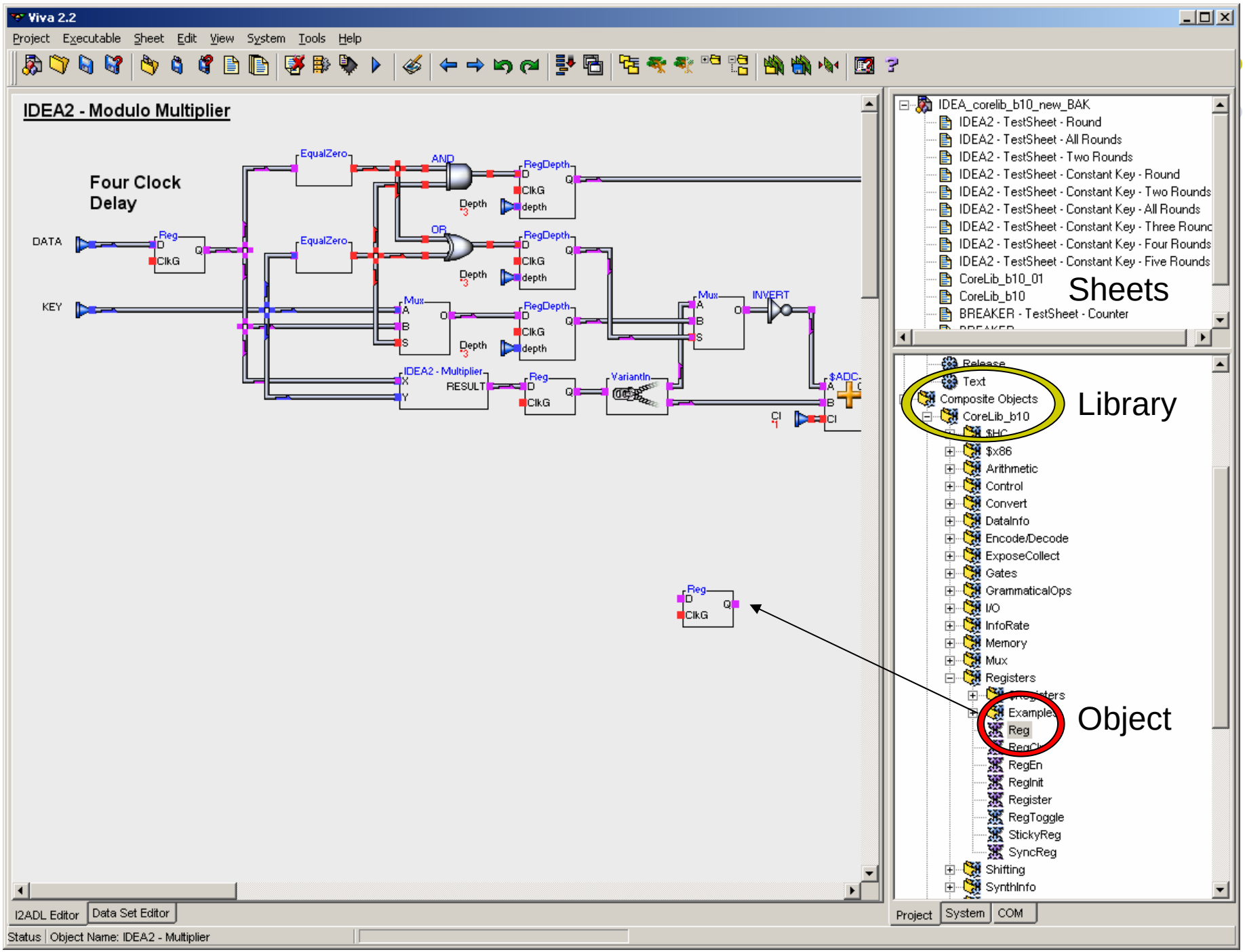


Star Bridge Hardware Architecture

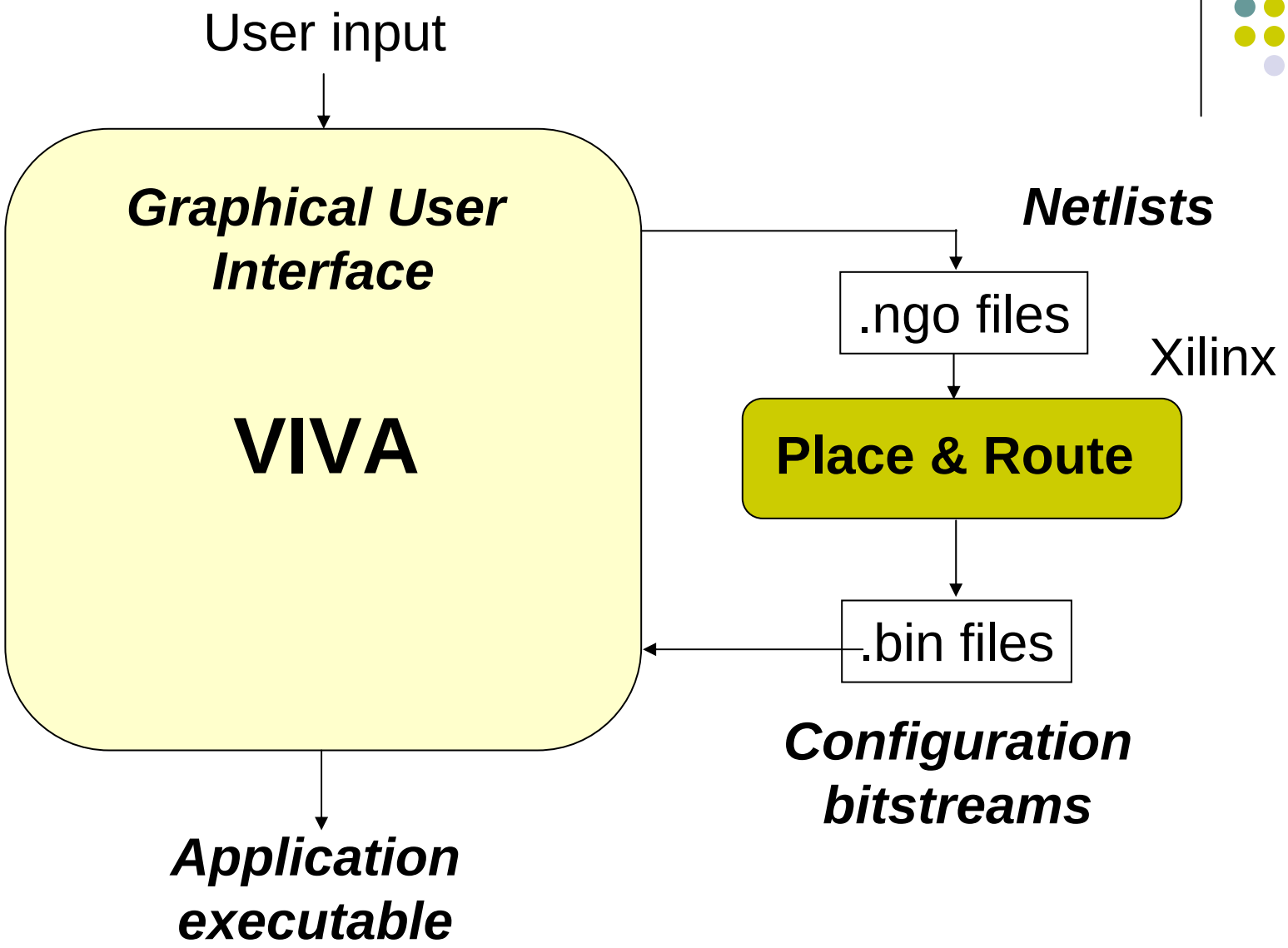


Star Bridge Processing Element (PE)

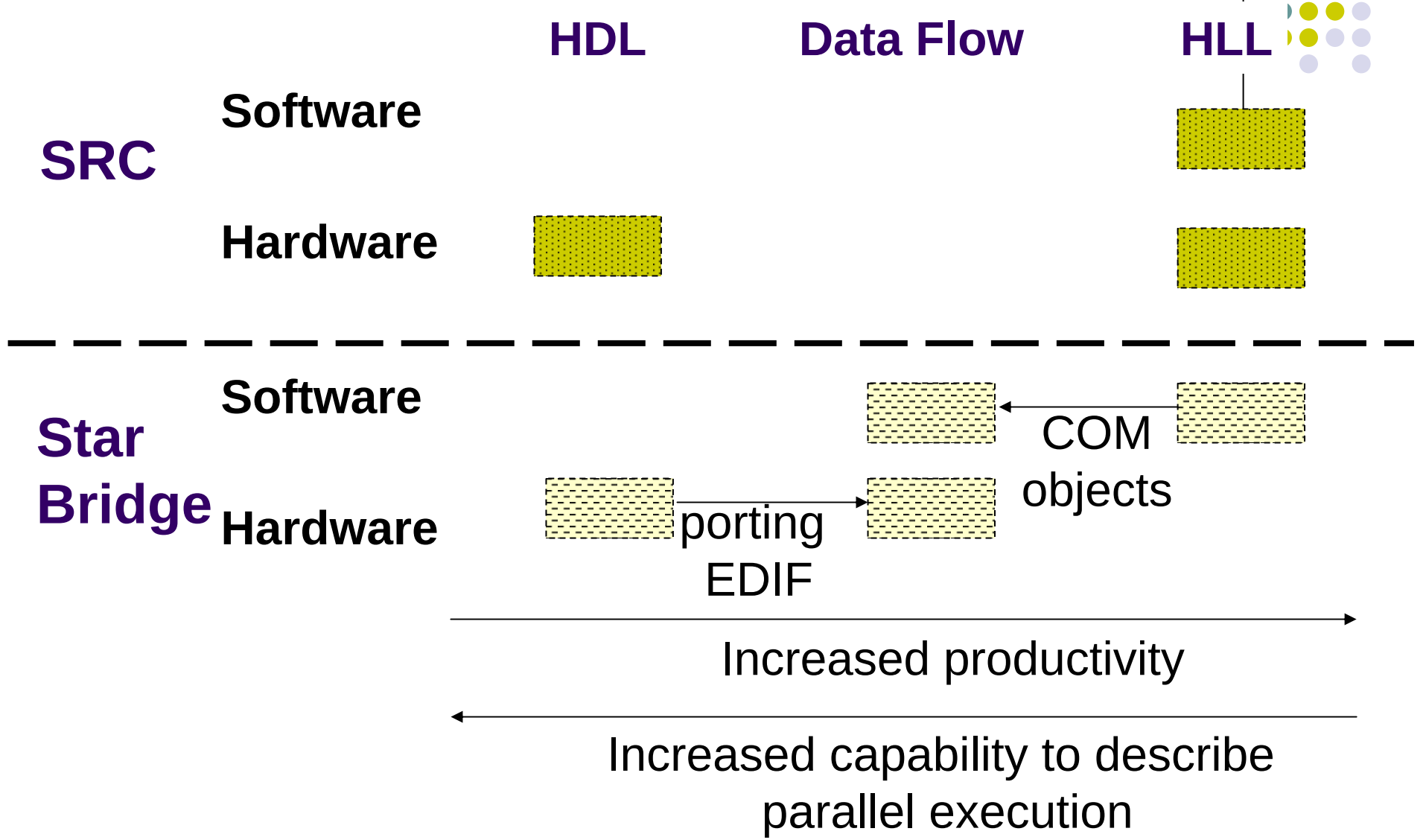


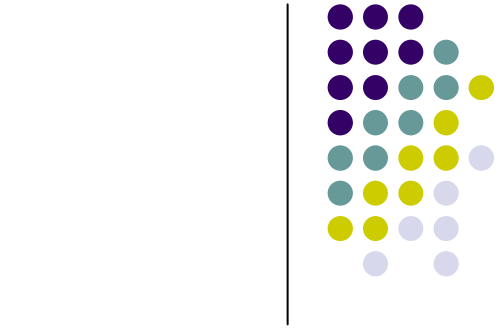

Viva 2.2
Project Executable Sheet Edit View System Tools Help
IDEA2 - Modulo Multiplier
Four Clock Delay
DATA
KEY
Reg
EqualZero
AND
OR
RegDepth
Depth
Mux
INVERT
IDEA2 - Multiplier
RESULT
VariantIn
$ADC
CI
IDEA_corelib_b10_new_BAK
IDEA2 - TestSheet - Round
IDEA2 - TestSheet - All Rounds
IDEA2 - TestSheet - Two Rounds
IDEA2 - TestSheet - Constant Key - Round
IDEA2 - TestSheet - Constant Key - Two Rounds
IDEA2 - TestSheet - Constant Key - All Rounds
IDEA2 - TestSheet - Constant Key - Three Rounc
IDEA2 - TestSheet - Constant Key - Four Rounds
IDEA2 - TestSheet - Constant Key - Five Rounds
CoreLib_b10_01
CoreLib_b10
BREAKER - TestSheet - Counter
Sheets
Release
Text
Composite Objects
CoreLib_b10
$x86
Arithmetic
Control
Convert
DataInfo
Encode/Decode
ExposeCollect
Gates
GrammaticalOps
I/O
InfoRate
Memory
Mux
Registers
Examples
Reg
RegEn
RegInit
Register
RegToggle
StickyReg
SyncReg
Shifting
SynthInfo
Library
Object
I2ADL Editor
Data Set Editor
Project
System
COM
Status
Object Name: IDEA2 - Multiplier

Star Bridge Compilation Process



SRC vs. Star Bridge Design Entry



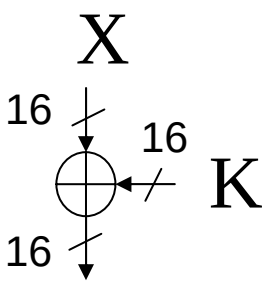


High-Throughput Secret-Key Encryption with IDEA

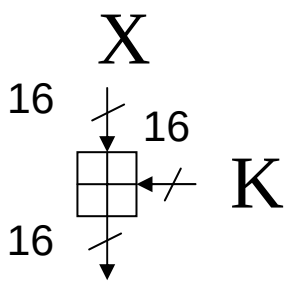
IDEA

- International Data Encryption Algorithm, published in 1990
- Conventional encryption algorithm suggested to replace DES
  - Largest use in PGP
- Block cipher
  - 128 bit key
  - 64 bit data block
  - 8 ½ rounds

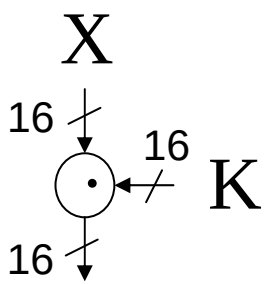
IDEA – Three Basic Operations



$$Y = X \oplus K$$



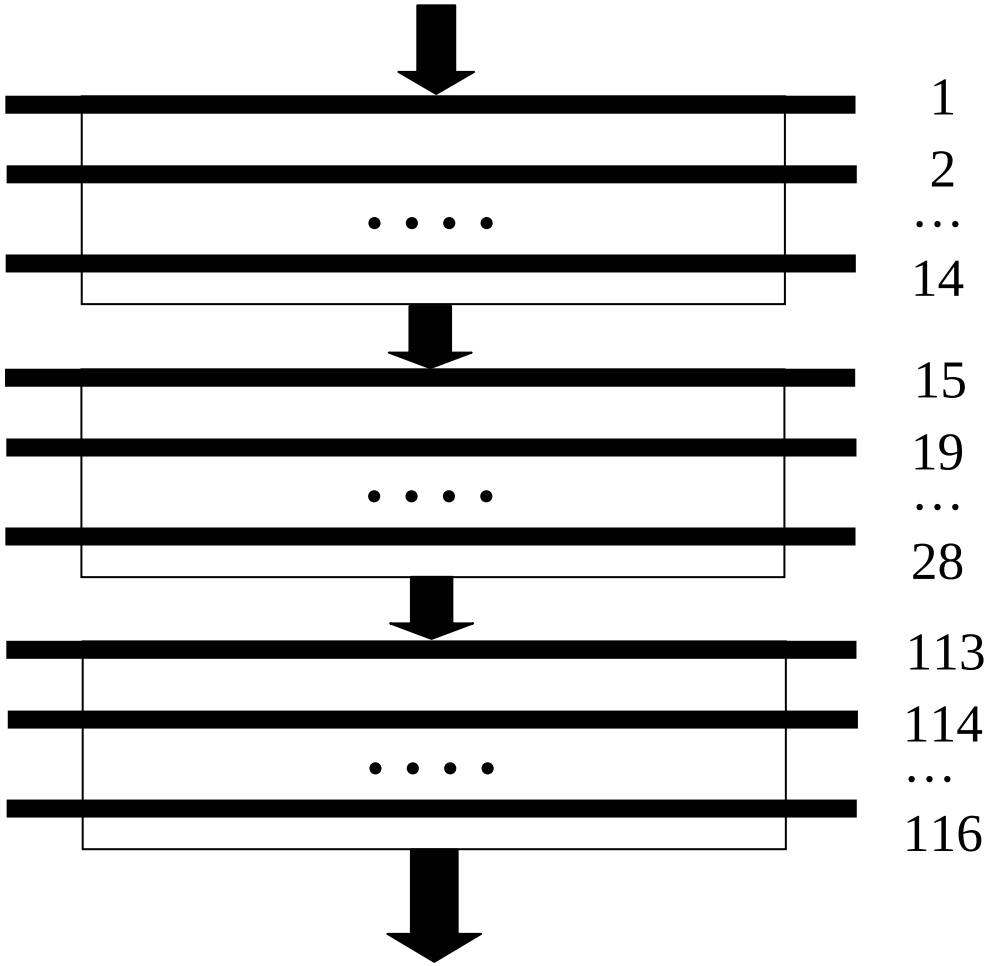
$$Y = X + K \bmod 2^{16}$$



$$Y = X \cdot K \bmod (2^{16}+1)$$

where 0 represents 2^{16}

Fully Pipelined Architecture of IDEA

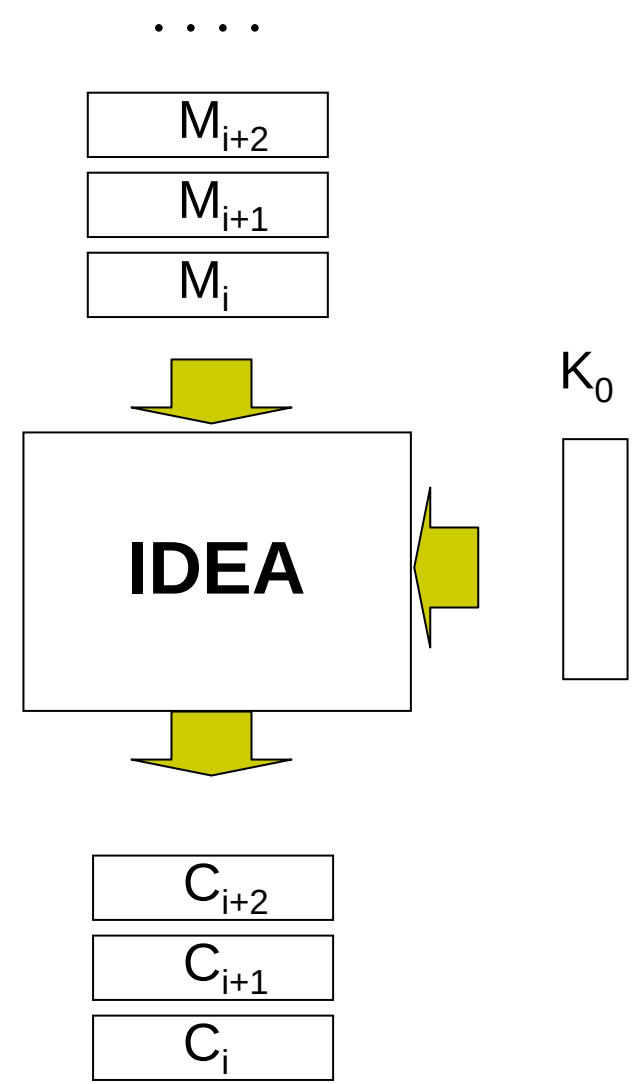


8.5 rounds

14 pipeline stages/round

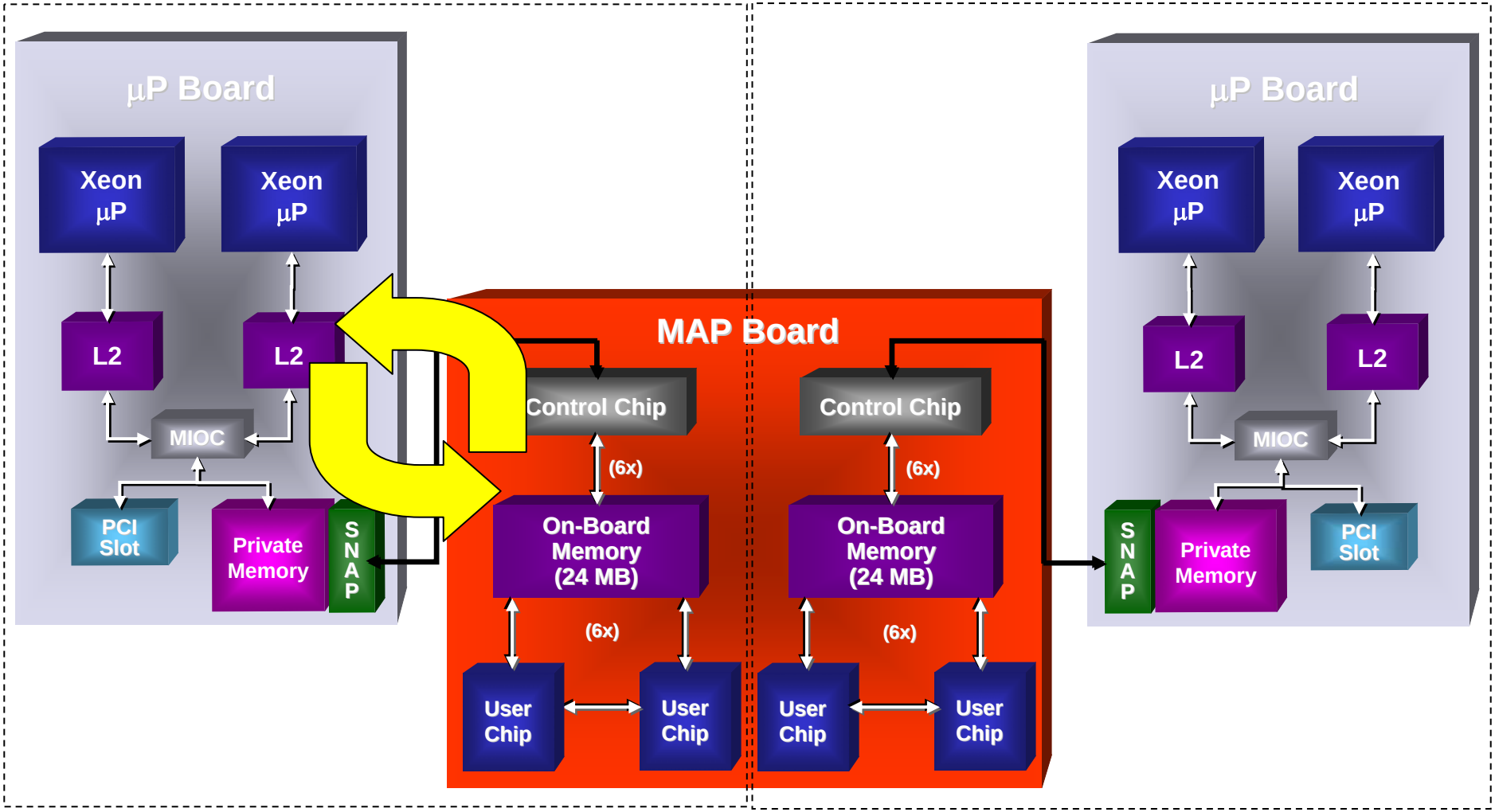
- **116 pipeline stages**
- **New input & new output every clock cycle**

High-Throughput Encryption

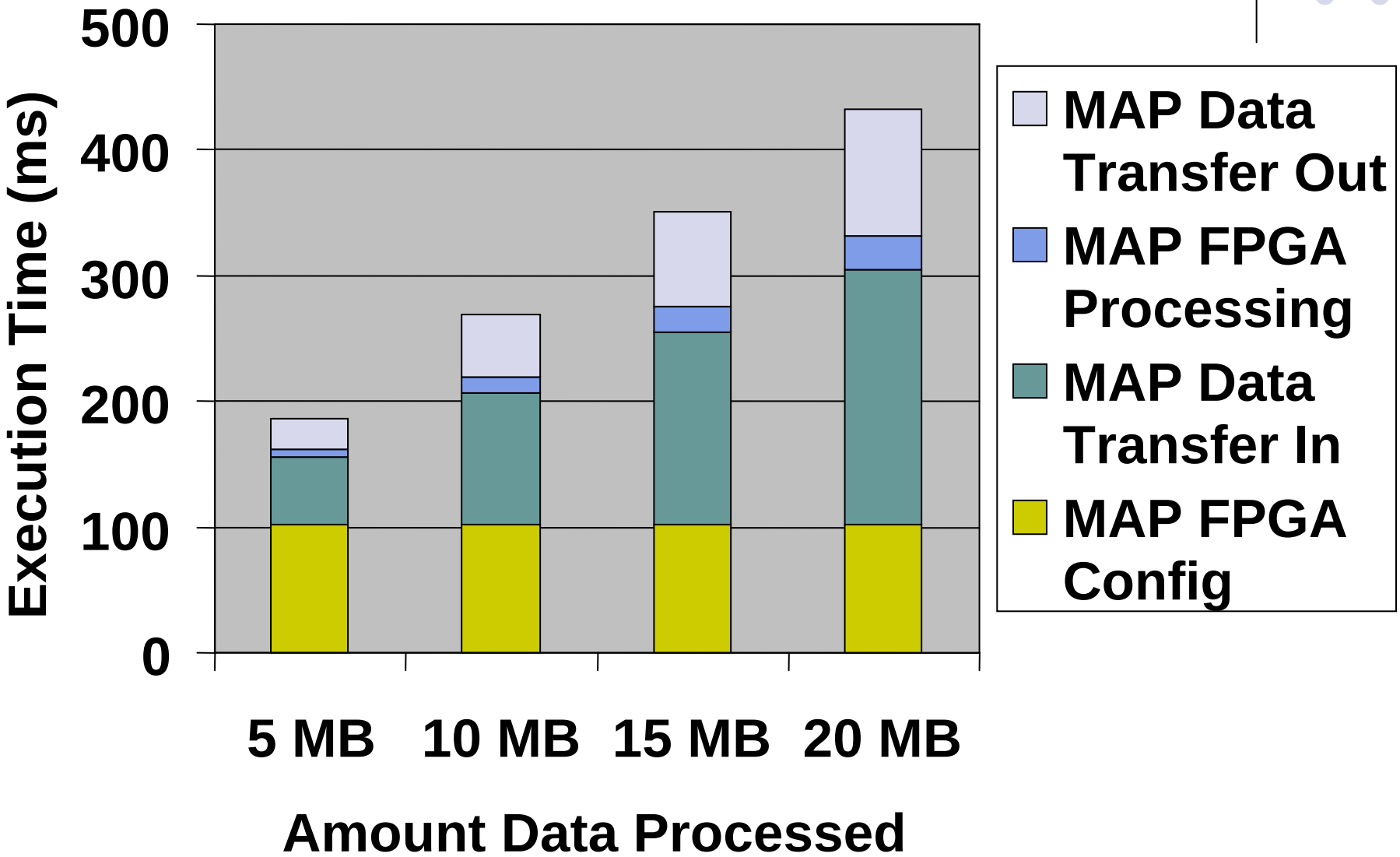


High-Throughput Secret-Key Encryption in SRC

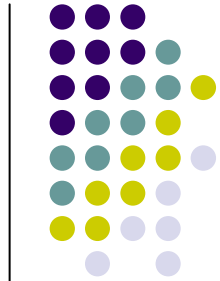
Data Flow During Encryption



IDEA Encryption



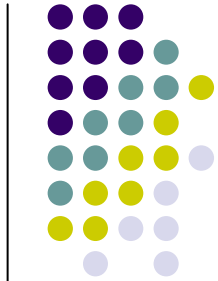
Problems



- **Execution time dominated by**
  - **Configuration of the MAP FPGA and**
  - **Data transfer between the System Common Memory and On-Board-Memory**

- **Configuration time hiding techniques**
  - **Preloading the configuration before execution**
  - **Flip-flopping FPGAs during reconfiguration**

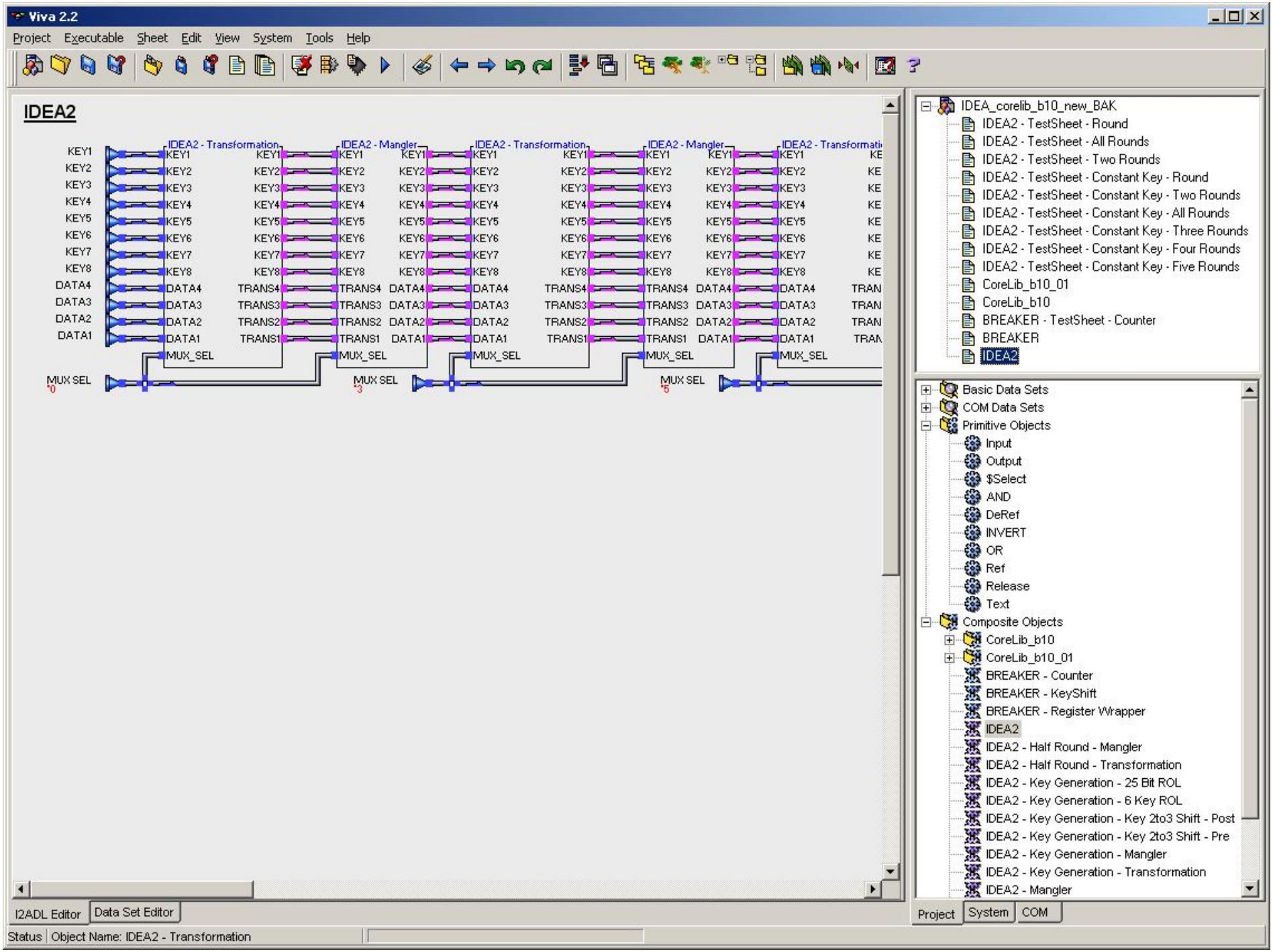
Comparison of SRC MAP vs. Pentium 4



Data Processed	**5MB**	**10MB**	**15MB**	**20MB**
SRC (sec)	0.08	0.17	0.25	0.33
Pentium 4 (sec)	7.99	15.96	23.94	31.93
SRC Speed-up	**95.60**	**95.16**	**96.27**	**96.53**

Pentium 4 implementation based on the Crypto++ 5.0 library

IDEA in VIVA


Viva 2.2
Project Executable Sheet Edit View System Tools Help
IDEA2
IDEA2 - Transformation
IDEA2 - Mangler
IDEA2 - Transformation
IDEA2 - Mangler
IDEA2 - Transformati
KEY1
KEY2
KEY3
KEY4
KEY5
KEY6
KEY7
KEY8
DATA4
DATA3
DATA2
DATA1
TRANS4
TRANS3
TRANS2
TRANS1
MUX_SEL
MUX SEL
*0
*3
*5
IDEA_corelib_b10_new_BAK
IDEA2 - TestSheet - Round
IDEA2 - TestSheet - All Rounds
IDEA2 - TestSheet - Two Rounds
IDEA2 - TestSheet - Constant Key - Round
IDEA2 - TestSheet - Constant Key - Two Rounds
IDEA2 - TestSheet - Constant Key - All Rounds
IDEA2 - TestSheet - Constant Key - Three Rounds
IDEA2 - TestSheet - Constant Key - Four Rounds
IDEA2 - TestSheet - Constant Key - Five Rounds
CoreLib_b10_01
CoreLib_b10
BREAKER - TestSheet - Counter
BREAKER
IDEA2
Basic Data Sets
COM Data Sets
Primitive Objects
Input
Output
$Select
AND
DeRef
INVERT
OR
Ref
Release
Text
Composite Objects
CoreLib_b10
CoreLib_b10_01
BREAKER - Counter
BREAKER - KeyShift
BREAKER - Register Wrapper
IDEA2
IDEA2 - Half Round - Mangler
IDEA2 - Half Round - Transformation
IDEA2 - Key Generation - 25 Bit ROL
IDEA2 - Key Generation - 6 Key ROL
IDEA2 - Key Generation - Key 2to3 Shift - Post
IDEA2 - Key Generation - Key 2to3 Shift - Pre
IDEA2 - Key Generation - Mangler
IDEA2 - Key Generation - Transformation
IDEA2 - Mangler
I2ADL Editor
Data Set Editor
Project
System
COM
Status
Object Name: IDEA2 - Transformation

Star Bridge Results

- Hardware interface and software support for efficient data transfer still under development
- Unable to measure end-to-end time without file i/o, data transfer in time, or data transfer out time
- MAP FPGA Processing Time the same as on the SRC machine

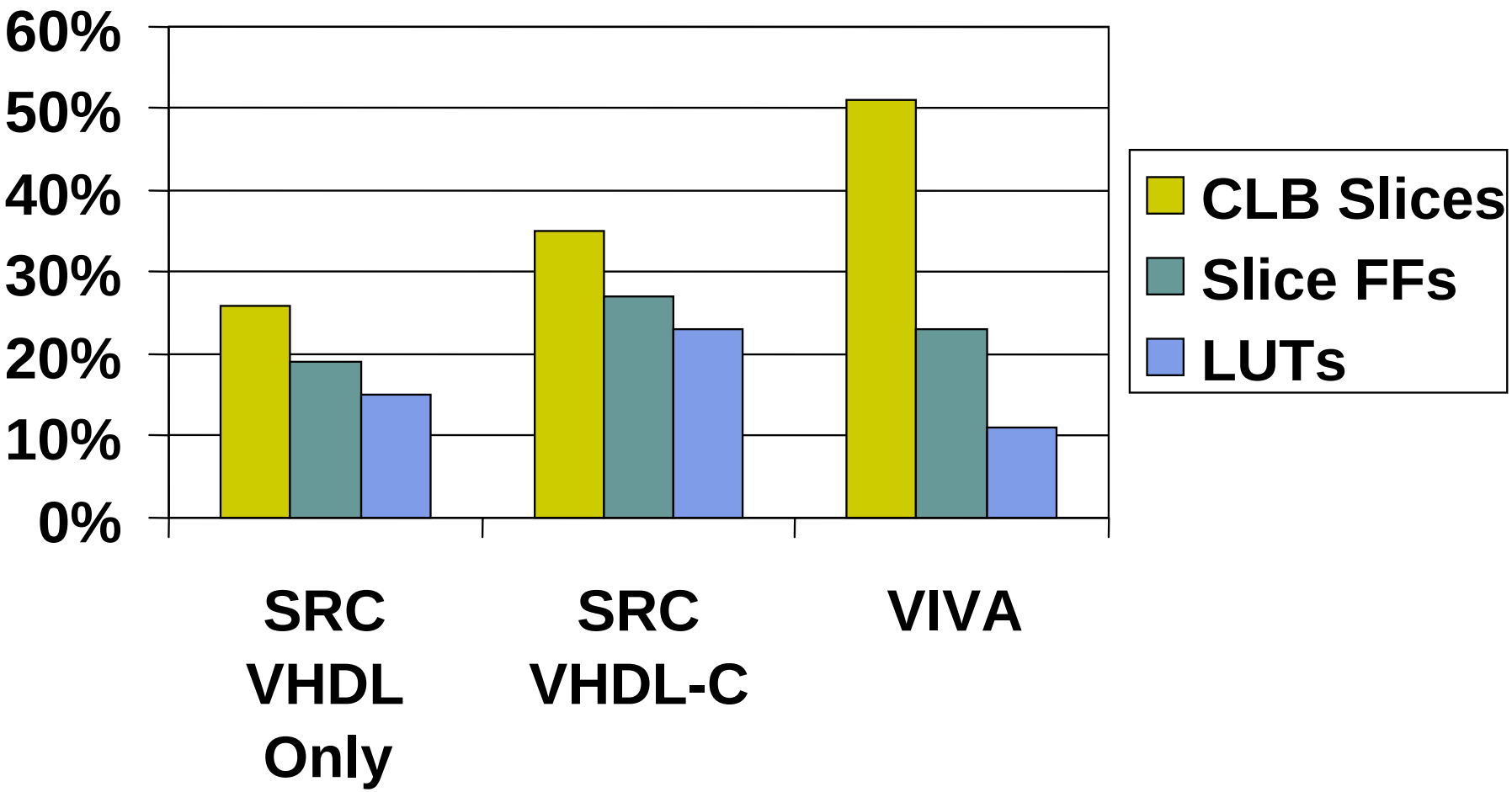
Results Comparison

IDEA – Compilation Time

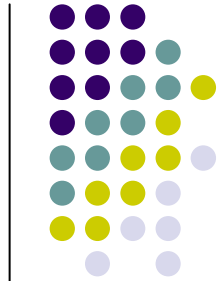
- SRC
  - Synthesis 2 min
  - Mapping 4 min
  - Placing and Routing 1 hr 34 min
- Star Bridge
  - Viva compilation time ~36 hrs
  - Mapping 14 min
  - Placing and Routing 1 hr 25 min

IDEA Use of FPGA Resources

Xilinx XC2V6000

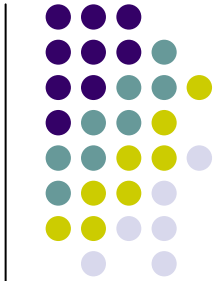


IDEA – Timing



- FPGA Processing Time the same in both systems
  - The same number of clock cycles
  - The same maximum clock frequency – 100 MHz
- The End-to-End time much smaller in SRC,
  but the exact comparison impossible because
  of the early development stage of the Star Bridge hardware and software

Conclusions



- Both platforms are unique expansions of existing paradigms
- FPGA data transfer is a significant bottleneck

  for I/O intensive applications, such as encryption
- SRC hardware and software more advanced

  Star Bridge system still in early development state
- Two order-of-magnitude speedup versus software-only solution for the high-speed IDEA encryption on SRC