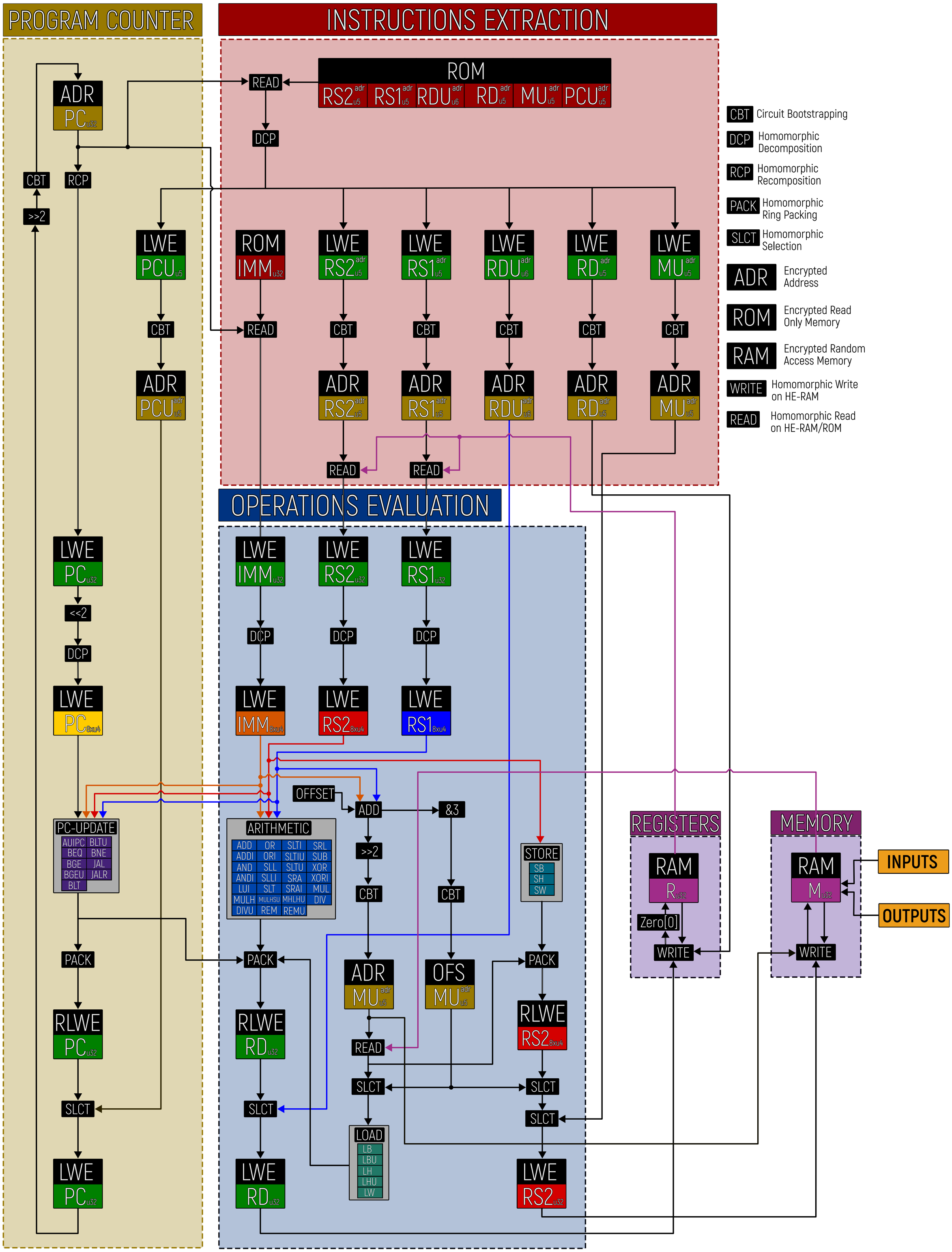
PROGRAM COUNTER
INSTRUCTIONS EXTRACTION
ROM
RS2 RS1 RDU RD MU PCU
READ
DCP
ADR
PC
CBT
RCP
>>2
LWE
PCU
ROM
IMM
LWE
RS2
LWE
RS1
LWE
RDU
LWE
RD
LWE
MU
CBT
READ
ADR
PCU
ADR
RS2
ADR
RS1
ADR
RDU
ADR
RD
ADR
MU
OPERATIONS EVALUATION
LWE
PC
<<2
DCP
LWE
PC
LWE
IMM
LWE
RS2
LWE
RS1
LWE
IMM
LWE
RS2
LWE
RS1
OFFSET
ADD
&3
>>2
CBT
PC-UPDATE
AUIPC BLTU
BEQ BNE
BGE JAL
BGEU JALR
BLT
ARITHMETIC
ADD OR SLTI SRL
ADDI ORI SLTIU SUB
AND SLL SLTU XOR
ANDI SLLI SRA XORI
LUI SLT SRAI MUL
MULH MULHSU MHLHU DIV
DIVU REM REMU
STORE
SB
SH
SW
PACK
RLWE
PC
SLCT
LWE
PC
PACK
RLWE
RD
SLCT
LWE
RD
ADR
MU
READ
SLCT
LOAD
LB
LBU
LH
LHU
LW
OFS
MU
PACK
RLWE
RS2
SLCT
SLCT
LWE
RS2
REGISTERS
RAM
R
Zero[0]
WRITE
MEMORY
RAM
M
WRITE
INPUTS
OUTPUTS
CBT Circuit Bootstrapping
DCP Homomorphic Decomposition
RCP Homomorphic Recomposition
PACK Homomorphic Ring Packing
SLCT Homomorphic Selection
ADR Encrypted Address
ROM Encrypted Read Only Memory
RAM Encrypted Random Access Memory
WRITE Homomorphic Write on HE-RAM
READ Homomorphic Read on HE-RAM/ROM