**1. Matrix Multiplication ISA & Microarchitecture**

**Profile Highlights**

* **Loads** ≈ 32 % (heavy streaming of matrix elements)
* **Calls & Constants** ≈ 18 % (loop overhead and function dispatch)
* **Arithmetic** ≈ 6.5 % (multiply‑add operations)

**Key ISA Features**

1. **Wide SIMD / FMA**
   * 256‑ or 512‑bit vector registers (V0…V15)
   * Fused‑Multiply‑Add instruction:  
     VFMADD.vv vd, vs1, vs2
2. **Strided & Block Loads**
   * Gather/Scatter with programmable stride:  
     VLOAD.vs vd, [base], stride, count
   * Tile‑based loads into on‑chip buffer
3. **Software‑Managed Scratchpad**
   * Explicit tile buffer instructions:  
     SPM\_LOAD tile\_reg, DRAM\_addr  
     SPM\_STORE tile\_reg, DRAM\_addr
4. **Non‑Blocking Prefetch**
   * PREFETCH [addr, stride] hides DRAM latency
5. **Zero‑Overhead Hardware Loops**
   * Loop registers + instruction:  
     LOOP LP\_COUNT, label
6. **Register File & Pipelines**
   * 32 vector + 32 scalar registers
   * Dedicated FMA pipelines: one 256‑bit FMA/cycle

**2. QuickSort ISA & Microarchitecture**

**Profile Highlights**

* **Loads** ≈ 28 % (array accesses)
* **Branches & Comparisons** ≈ 10 % (partition logic and recursion)
* **Calls & Stack Ops** ≈ 7–9 % (function recursion)

**Key ISA Features**

1. **Predicated / Conditional Moves**
   * CMOV.GT rd, rs, rt ; rd = (rs > rt)? rs : rt
   * Reduces mispredicted branches
2. **Hardware Stack Instructions**
   * PUSH rs1, rs2
   * POP rd1, rd2
   * Auto‑spill/fill on CALL/RET
3. **Advanced Branch Predictor**
   * Tournament predictor + loop‑buffer cache
   * Dedicated small BTB for tight loops
4. **Post‑Increment Addressing**
   * LDI rd, [rs1+], imm ; rd = M[rs1] ; rs1 += imm
5. **Link‑Register Calls**
   * CALL.R lr, addr
   * RET.R lr (zero‑overhead return)
6. **Small, Prefetching L1 Data Cache**
   * 16 – 32 KB with hardware prefetch

**3. AES Algorithm ISA & Microarchitecture**

**Profile Highlights**

* **Loads** ≈ 48 % (state & round keys)
* **Calls & Constants** ≈ 14 % (S‑box lookups, key schedule)
* **Bitwise Operations** ≈ 10 – 12 % (XOR, shifts, rotates)

**Key ISA Features**

1. **Dedicated AES Rounds**
   * AESENC rd, rs, rk ; one full round
   * AESDEC rd, rs, rk ; inverse round
2. **Carry‑Less Multiply & Byte‑Shuffle**
   * CLMUL rd, rs1, rs2 ; GF(2⁸) mixcolumns
   * PSHUFB vd, vs, imm8 ; byte‑level permutation
3. **128‑Bit SIMD Registers**
   * Hold full AES state in one register
   * Micro‑coded key schedule with assist opcodes
4. **On‑Chip LUT for S‑Box**
   * 256×8 bit RAM single‑cycle access
   * Prefetch round constants in CSR
5. **Fully Unrolled, Pipelined Rounds**
   * 10 rounds in microcode, no branch overhead
6. **Security Hardening**
   * Constant‑time primitives
   * Masking registers to prevent side‑channels

**4. Summary Comparison**

|  |  |  |  |
| --- | --- | --- | --- |
| **Feature** | **Matrix Multiplication** | **QuickSort** | **AES** |
| **Compute Units** | Wide SIMD + FMA pipelines | Scalar ALU + predicated ops | SIMD-width crypto co-processor |
| **Memory Model** | Scratchpad + strided loads | Cache + post-inc addressing | On‑chip S‑Box LUT + key caches |
| **Branch Handling** | Minimal | Advanced predictor | Fully unrolled (no branches) |
| **Special Instructions** | PREFETCH; LOOP | CMOV; PUSH/POP; LDI post‑inc | AESENC; CLMUL; PSHUFB |