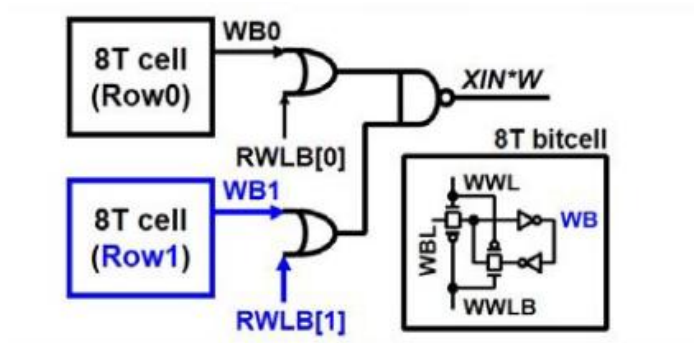
基于存算一体架构的后量子密码融合加速器

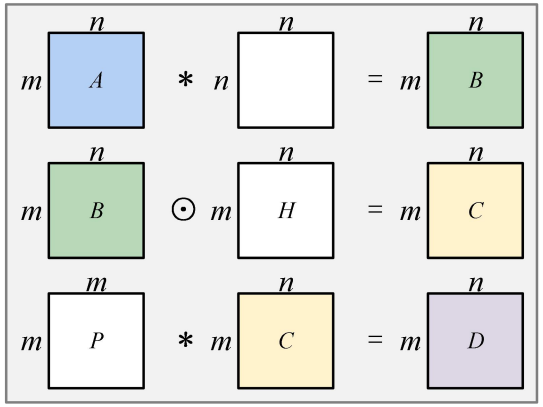
➢ 存算电路：粗粒度SRAM数字存算一体阵列

基本单元

粗粒度8T SRAM bitcell（DCIM）

乘法单元：2个8T bitcell + OAI，可同步读写



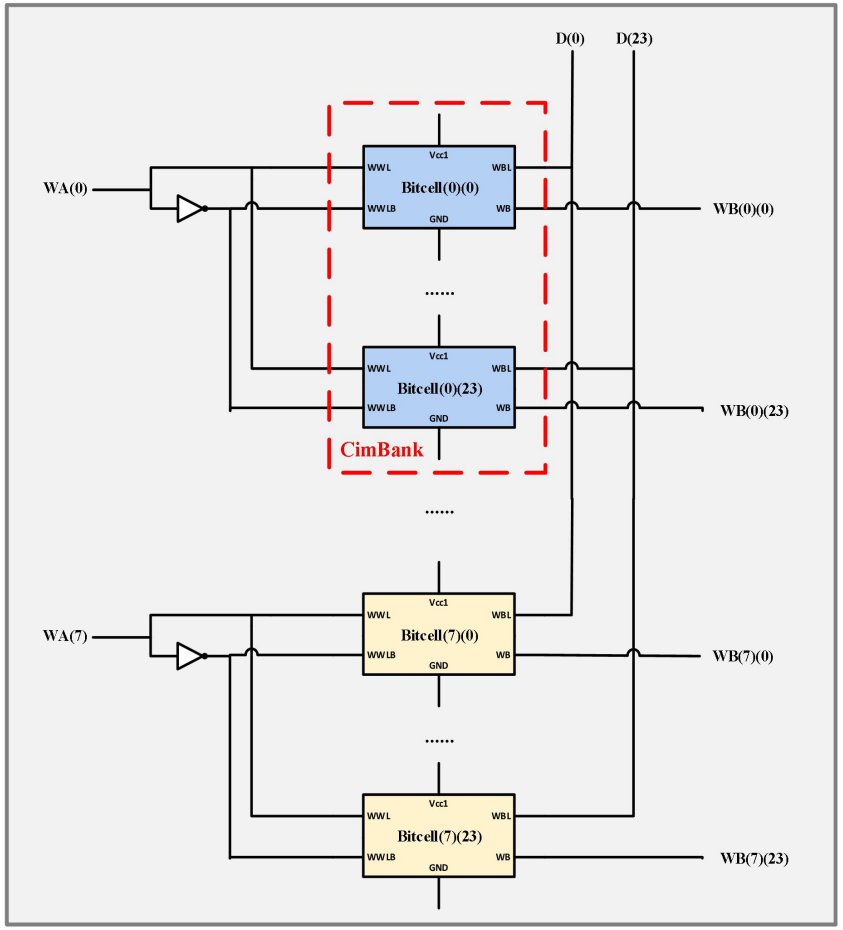


最小阵列

验证规模：$16 \times 8, 24bits\ (m = 16, n = 8)$

- Kyber：权重12bit；Dillithium：权重24bit

阵列连接

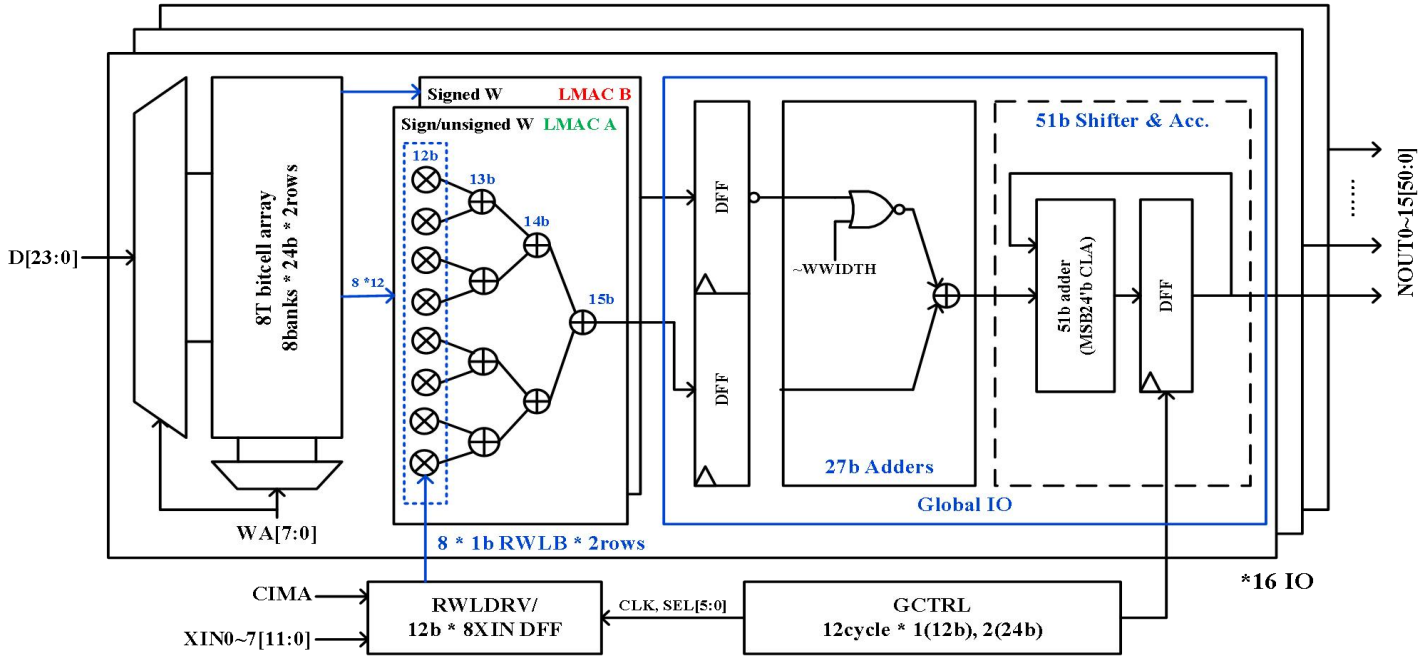


基于存算一体架构的后量子密码融合加速器

➢ 存算电路：可配置矩阵向量乘法电路 -> 近存结构

电路构成

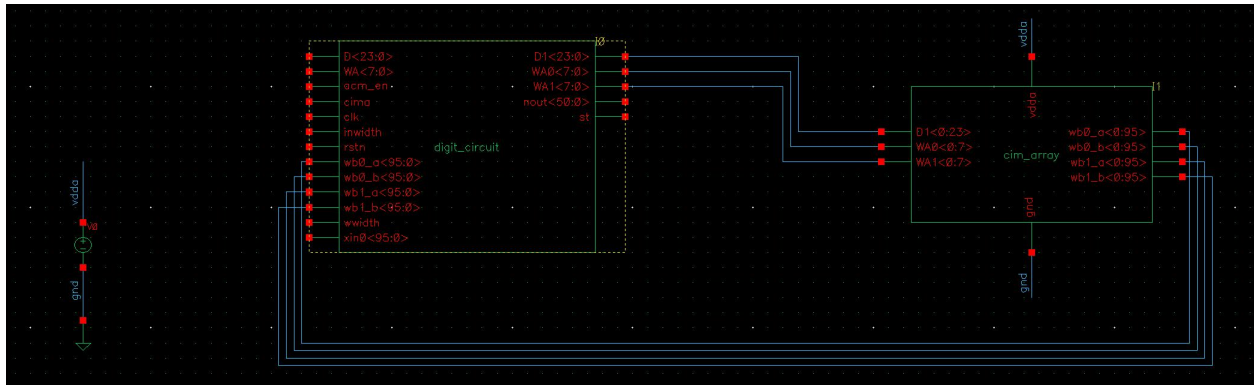
- CIM Array：16 IO * 8 banks * 24b * 2rows，写入/读出权重数据
- Local-MAC：通过OAI完成输入与权重乘法，并完成输出的8 * 12b的累加计算
- Global IO：DFF + adders + Shifter & Acc.，在多个时钟周期下完成多个单bit输入的累加
- RWLDRV + GCTRL：生成时序与控制信号，调节输入和累加的时序



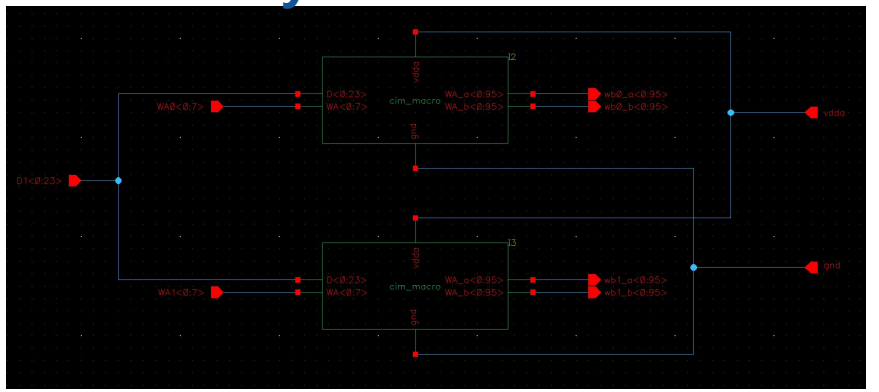
基于存算一体架构的后量子密码融合加速器

➢ 电路仿真：Virtuoso数模混合电路搭建（待仿真）

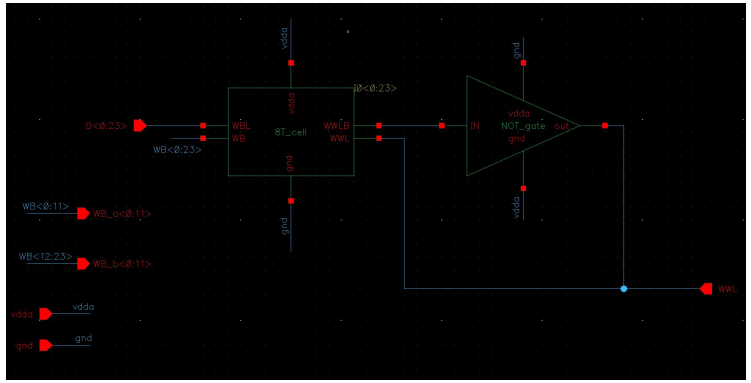
1. 电路整体



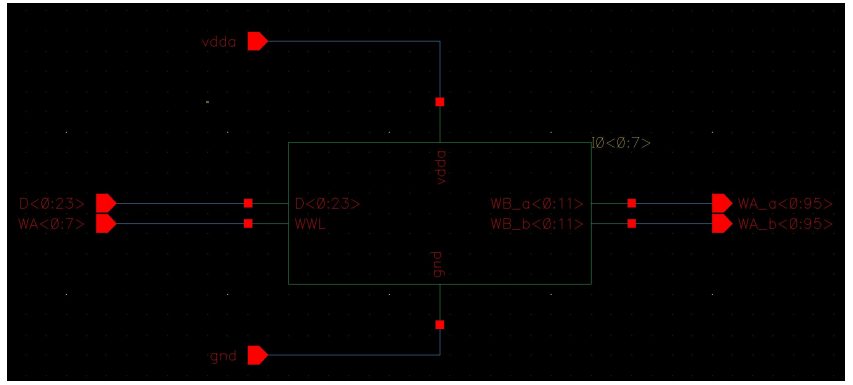
2. CimArray



3. CimMicro



4. CimBank



5. 8T Cell