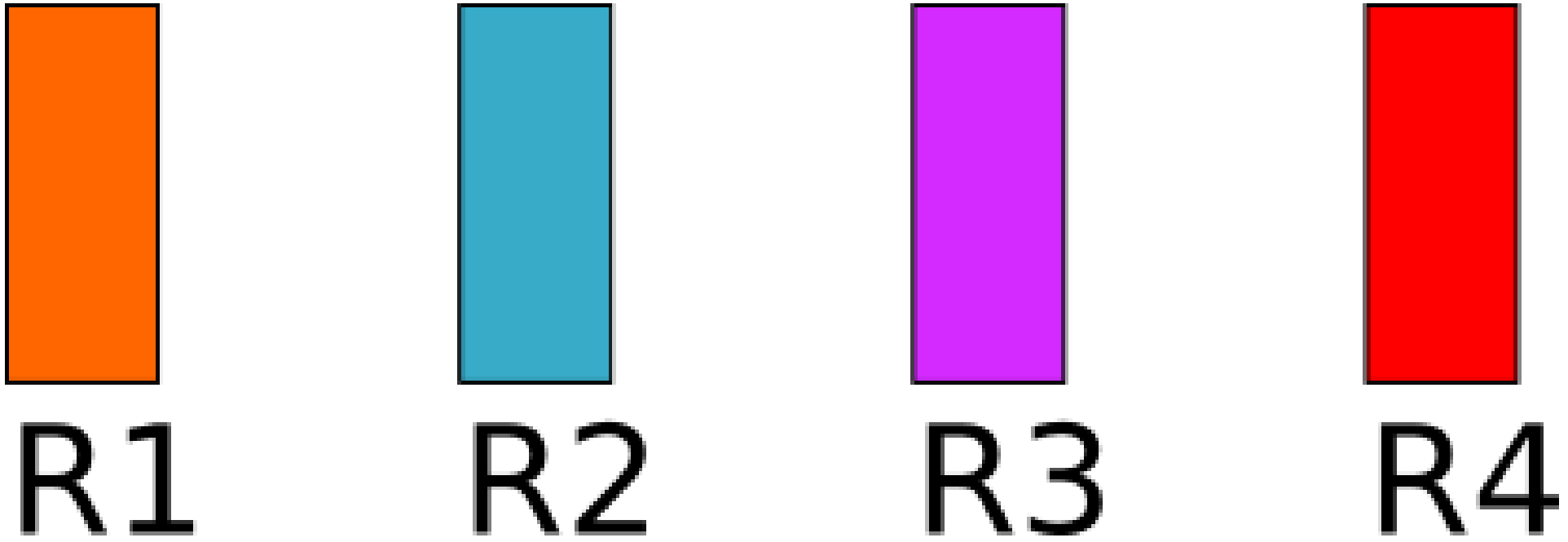
SHA1

- 160 bits
- 80 rounds
- 4 unique round types
- Round *n* output → round *n+1* input

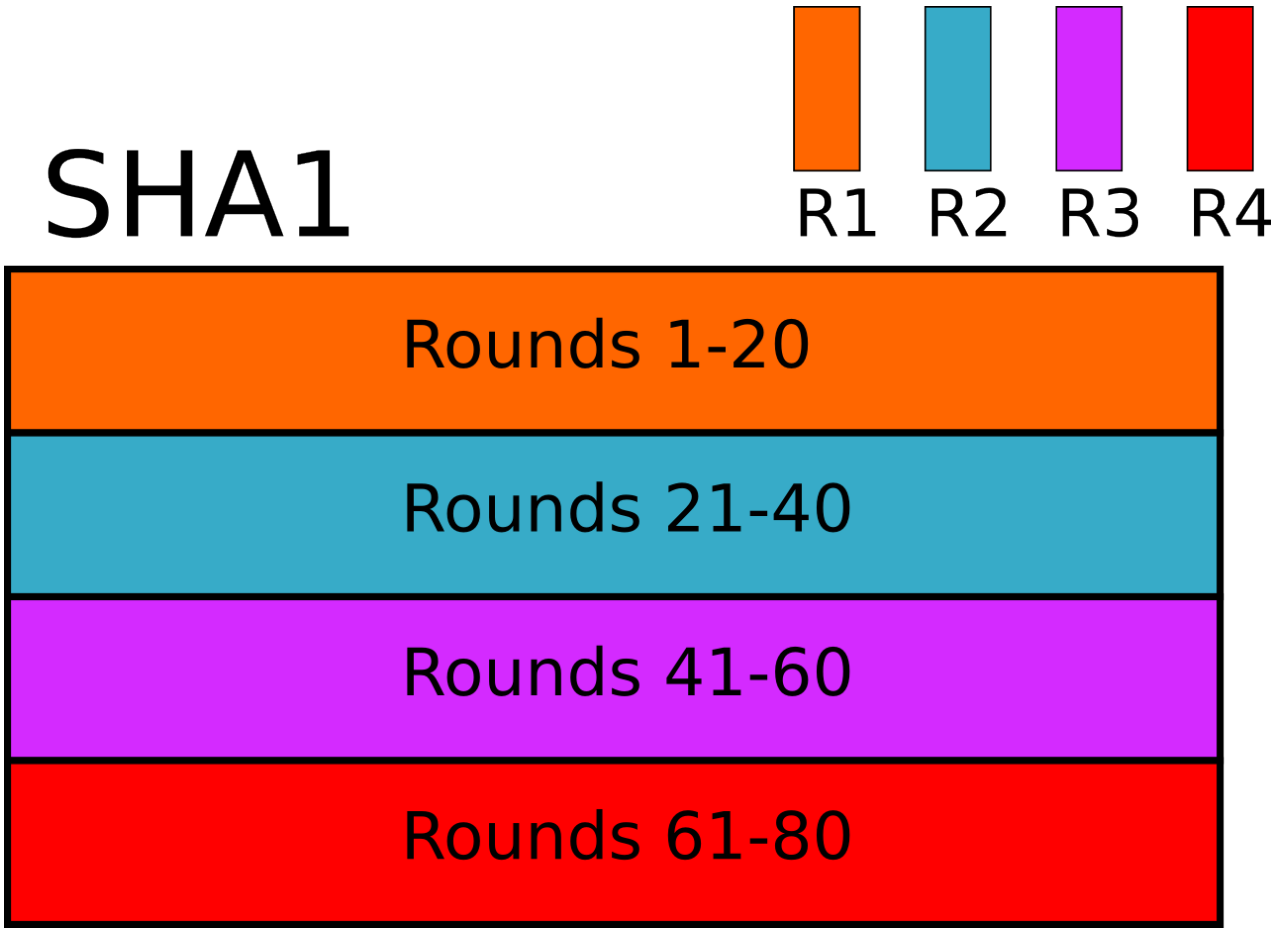
SHA1 ASIC

- Each round just a sequence of logic gates
- Logical implementation: *round per clock cycle*
- All about silicon real estate

SHA1 Rounds Visualised



SHA1 Rounds Visualised



AES-NI Instructions

Instruction	Description
AESENC	Perform one round of AES encryption
AESENCLAST	Perform last round of AES encryption
AESDEC	Perform one round of AES decryption
AESDECLAST	Perform last round of AES decryption
AESKEYGENASSIST	Assist in round key generation
AESIMC	Assist in inverse mix columns
PCLMULQDQ	Carryless multiply

Performance: 3.5 cycles per byte
≈ 56 cycles per block
≈ 760MB/s (@2.8Ghz)

Source: http://en.wikipedia.org/wiki/AES_instruction_set