A Comparison of AES Candidates on the Alpha 21264

- Richard Weiss
  Compaq Computer Corp
  Shrewsbury, MA
- Nathan Binkert
  Computer Science Dept
  University of Michigan
  Ann Arbor, MI

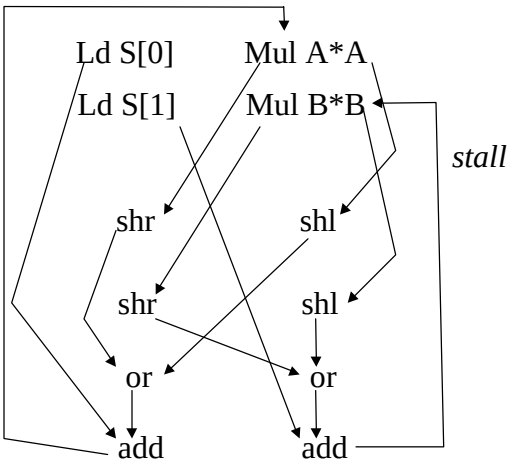
The Alpha 21264

- Can issue 4 integer instructions/cycle
- 64-bit data path
- Latency for an integer multiply is 7, can issue one/cycle
- no 32-bit rotate
- can only do two shifts/cycle

Encrypting Multiple Streams

- Multiple independent blocks
- Single processor
- Single program
- Can better utilize the resources on superscalar processors by processing multiple streams in parallel

Dependency graph



Two stream

Ld S[0]	Mul A*A		
Ld S[1]	Mul B*B		
		shr	shl
		shr	shl
		or	or
		add	add
		Ld S[0]	Mul A*A
		Ld S[1]	Mul B*B
shr	shl		
shr	shl		
or	or		
add	add		

Methodology

- Brian Gladman's code
- cycle counter
- 128-bit key encryption
- For multistream, modified C-code
- Assembly code (Rijndael, Twofish, RC6) to estimate max single stream performance

Single Stream Timing

21164	Mars	RC6	Rijndael	Serpent	Twofish
Ours	701c	571c	439c	984c	442c
Granboulan website	507c	559c	490c	998c	490c

21264	Mars	RC6	Rijndael	Serpent	Twofish
Ours	515c	428c	293c	854c	316c
Granboulan website	450c	382c	285c	855c	315c

IPC analysis

21264	Mars	RC6	Rijndael	Serpent	Twofish
Inst	968	660	755	1863	876
Cycles	507	383	285	850	316
IPC	1.9	1.7	2.6	2.2	2.8

Two Stream Timing

21264	Mars	RC6	Rijndael	Serpent	Twofish
Cycles	445	326	293	550	316
Speedup	1.1	1.2	1.0	1.5	1.0

Conclusions

- Increasing issue width alone has limited gain for single stream applications.
- Multistream applications can better use these resources in some cases.
- Multistream paradigm can cover instruction latency.