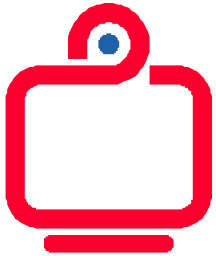
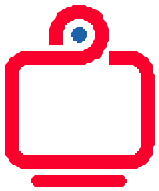


Performance of AES Candidates on the TriMedia VLIW Media-processor

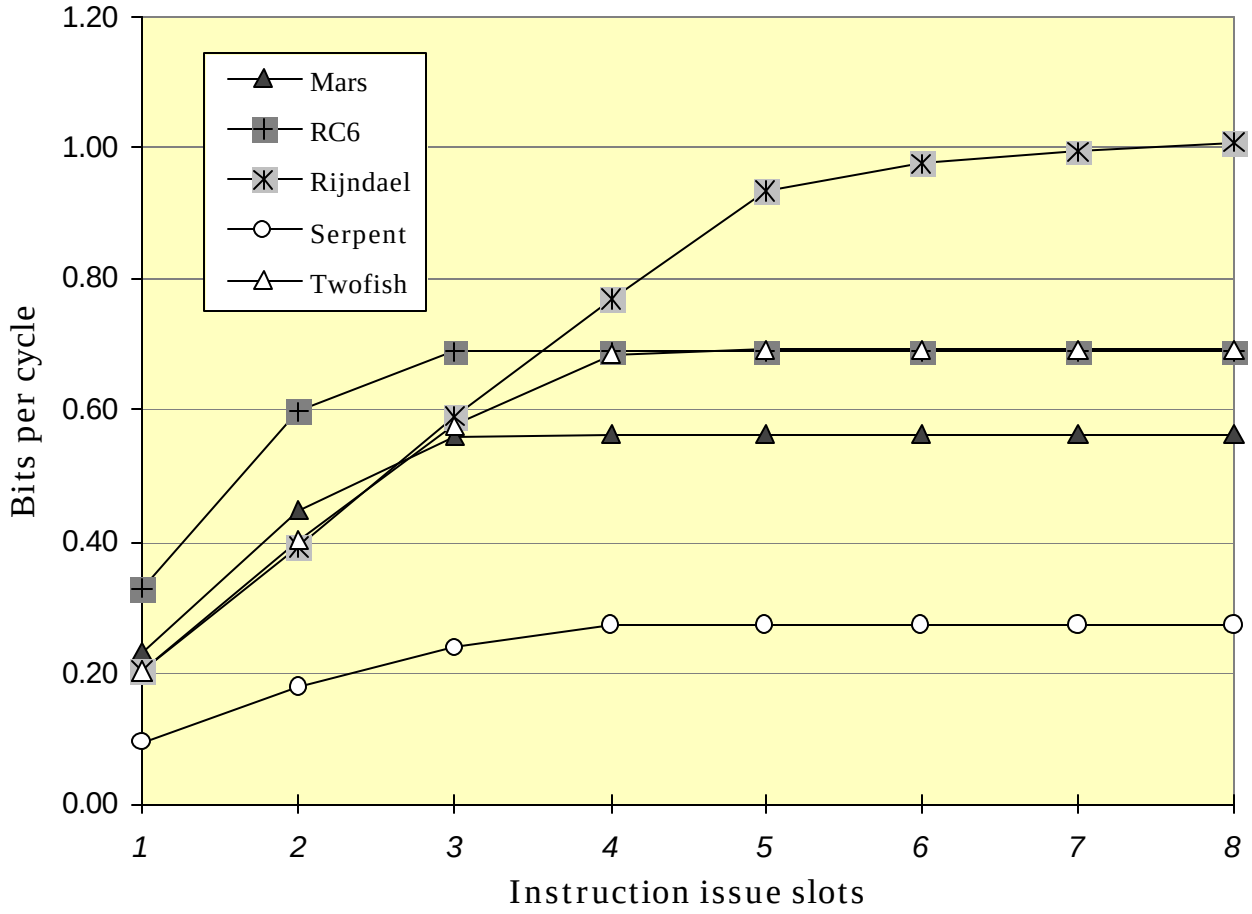
- 3rd AES Candidate Conference, New York, April 2000

Craig Clapp

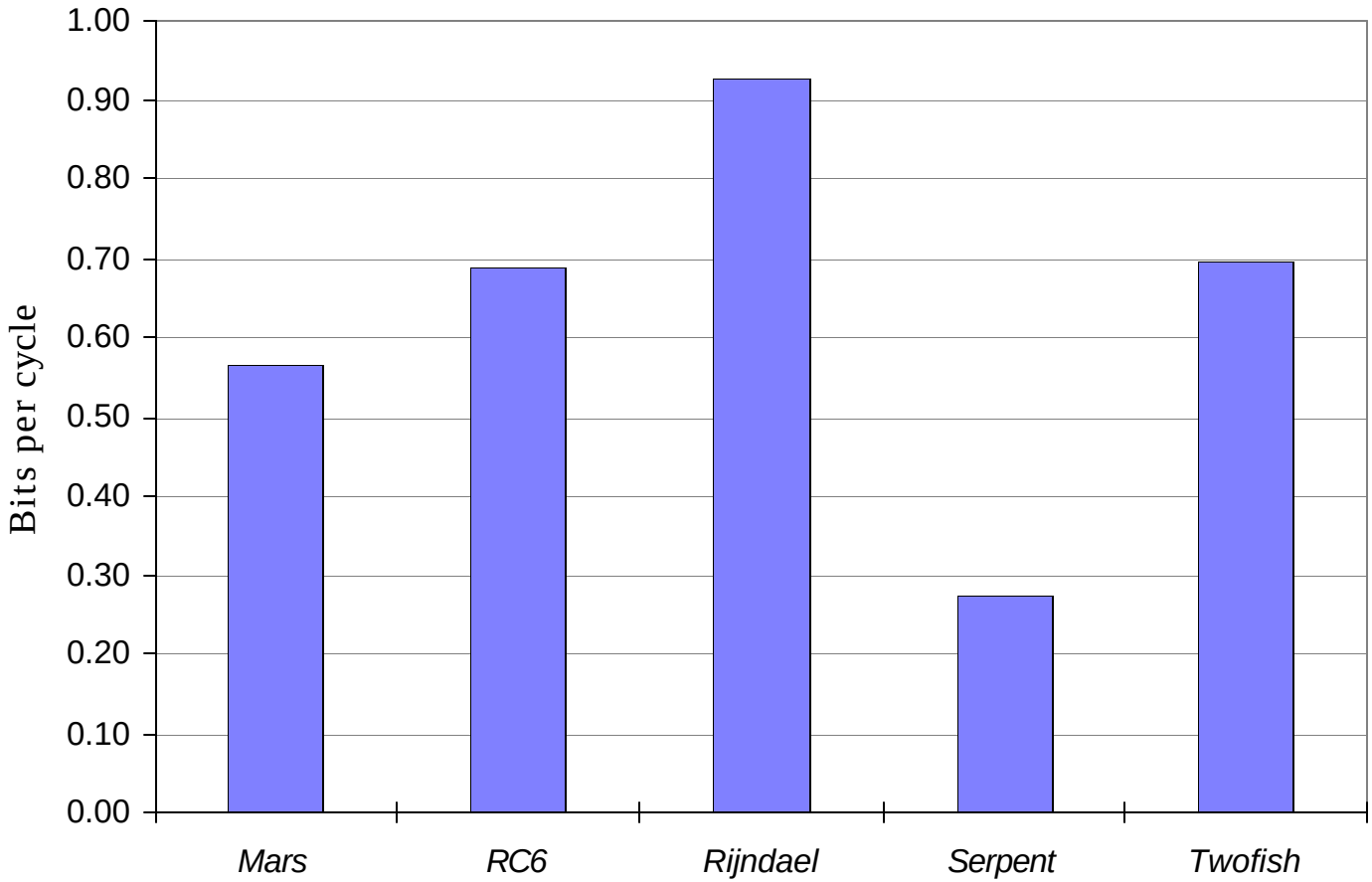
PictureTel Corporation



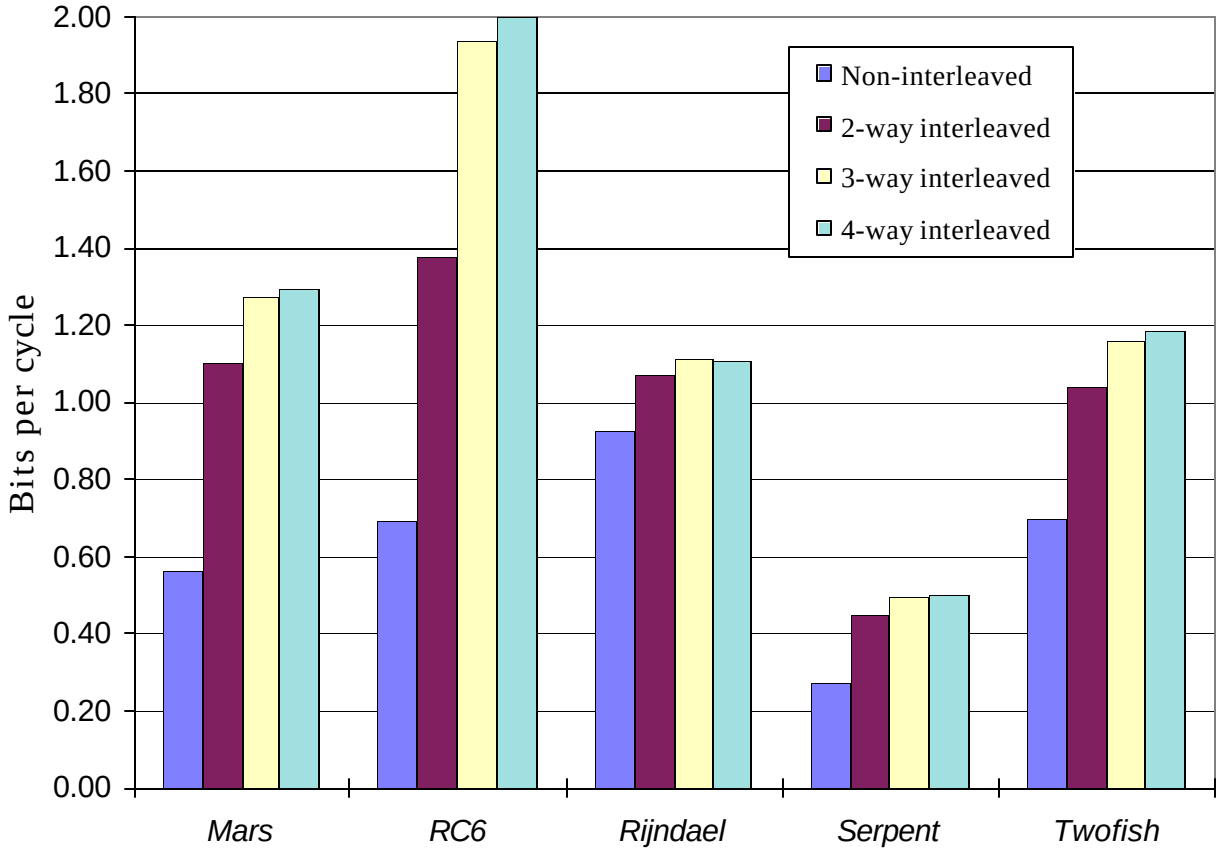
AES candidate performance versus execution resources (theoretical)



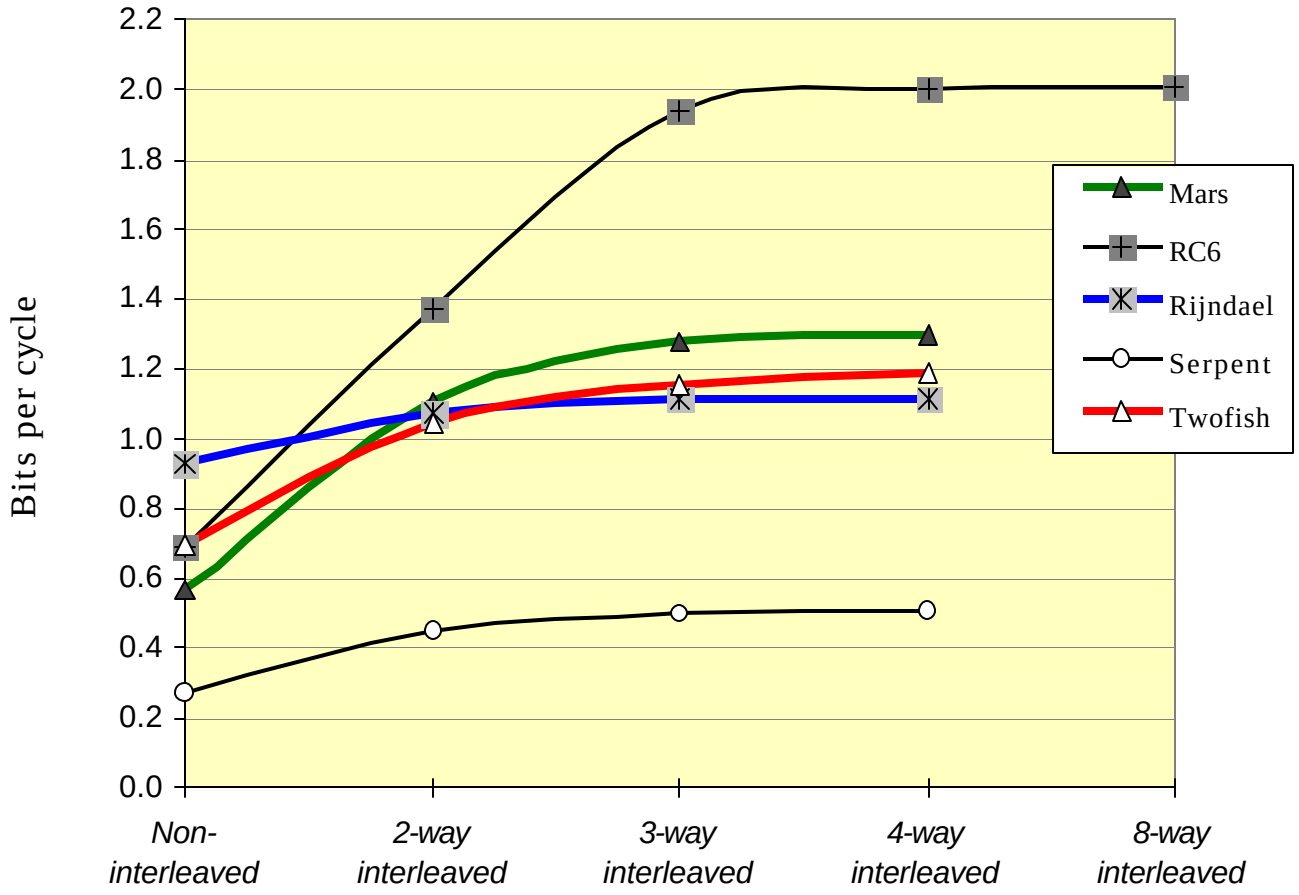
Throughput of AES candidates on TriMedia CPU in feedback mode

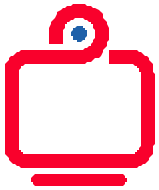


Throughput of AES candidates on TriMedia CPU in interleaved modes



Throughput of AES candidates on TriMedia CPU in interleaved modes





Conclusions

- On advanced CPUs the relative performance of candidates may ***differ wildly*** between feedback and non-feedback (or interleaved) modes
- Rijndael's performance varies the least with mode
- RC6 shows the greatest benefit from interleaved modes, considerably outperforming the other candidates