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

![Bar chart showing throughput comparison]

- Mars
- RC6
- Rijndael
- Serpent
- Twofish
Throughput of AES candidates on TriMedia CPU in interleaved modes

![Diagram showing throughput of AES candidates on TriMedia CPU in interleaved modes.](image-url)
Throughput of AES candidates on TriMedia CPU in interleaved modes

![Graph showing 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.