
hp
invent

AES

AES Finalists on PA-RISC and IA-64

Implementations and Performance

John Worley

HP Labs

AES3 Conference

May 15, 2000

AES

CPU Characteristics

PA-RISC

- **Out-of-order Superscalar**
- **Two Integer/Float, two Load/Store per cycle**

IA-64

- **Explicit parallelism (EPIC)**
- **Issue up to six operations per cycle**

AES

Programming Opportunities and Issues

PA-RISC

- **Straight-line coding, careful scheduling for best out-of-order performance**

IA-64

- **Large register file (128 integer) avoids memory traffic**
- **Rotating registers allow for compact, efficient loops**
- **Predication avoids branches and special-case code**
- **Fixed 32-bit Rotations require extra cycles**

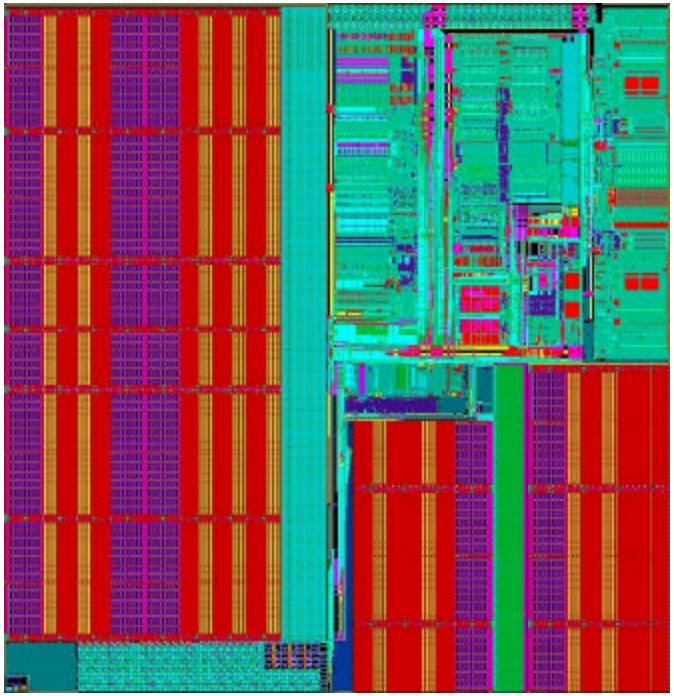
Common Difficulties

- **32x32 Multiplication**
- **Variable Rotations**

AES

PA-RISC Performance

- **Routines timed with 64-bit cycle counter**
- **Timed 100,000 random inputs 10,000 times each, taking the *minimum* run time for each input**
- **Results form a distribution!**



PA-8500

AES

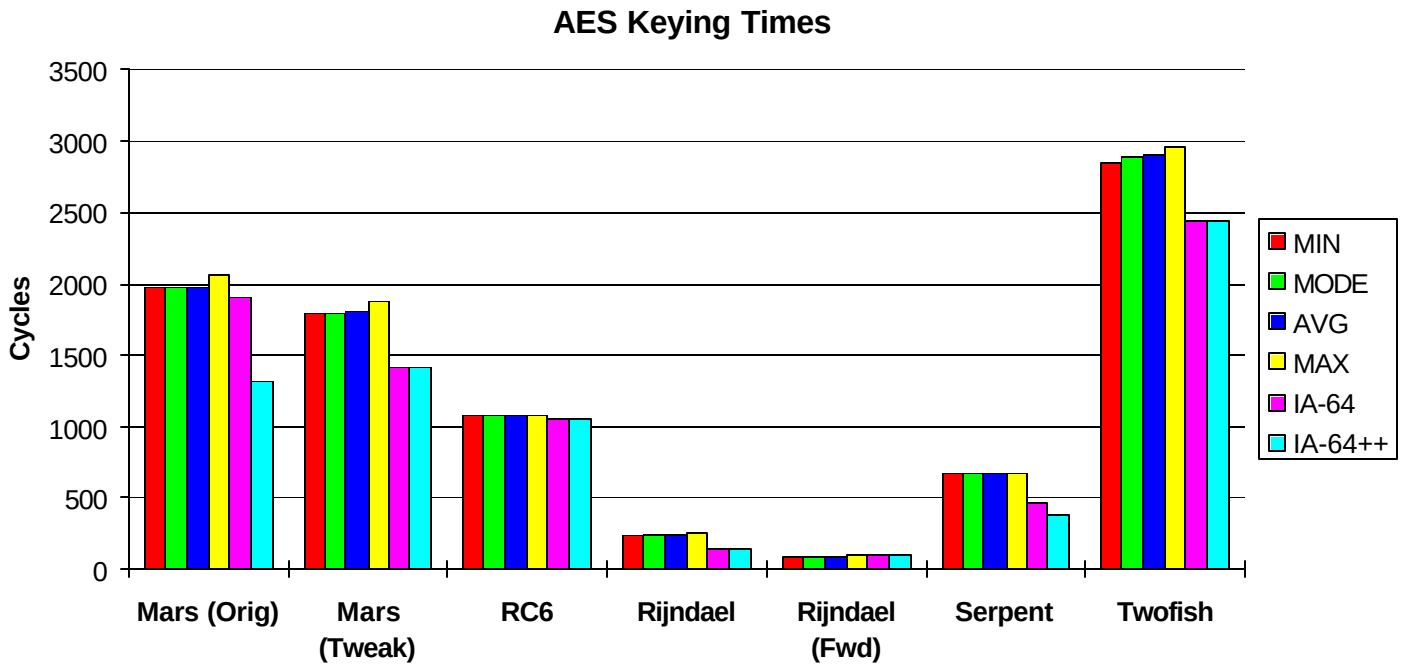
PA-RISC Performance

Keying Distributions

	Min	Avg	Mode	Max	s
Mars	**1797**	**1804.65**	**1799**	**1879**	**8.97**
RC6	**1077**	**1077**	**1077**	**1077**	**0.00**
Rijndael	**239**	**249.25**	**249**	**261**	**2.43**
Serpent	**668**	**668.79**	**669**	**669**	**0.40**
Twofish	**2846**	**2901.79**	**2897**	**2964**	**16.73**

Time in cycles

PA-RISC Performance



AES

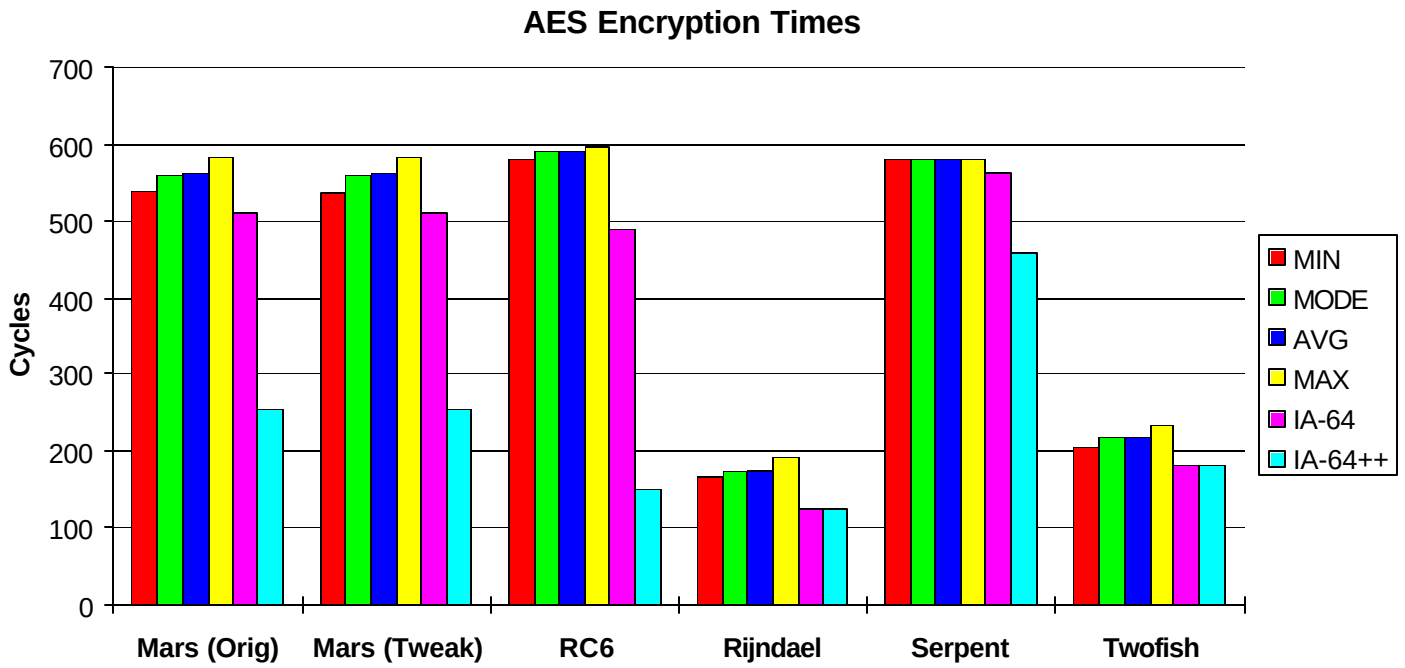
PA-RISC Performance

Encryption Distributions

	Min	Avg	Mode	Max	s
Mars	**538**	**561.87**	**560**	**584**	**7.05**
RC6	**580**	**590.76**	**591**	**597**	**1.24**
Rijndael	**168**	**175.5**	**174**	**193**	**2.74**
Serpent	**580**	**580**	**580**	**580**	**0.00**
Twofish	**205**	**217.45**	**217**	**233**	**2.93**

Time in cycles

PA-RISC Performance



AES

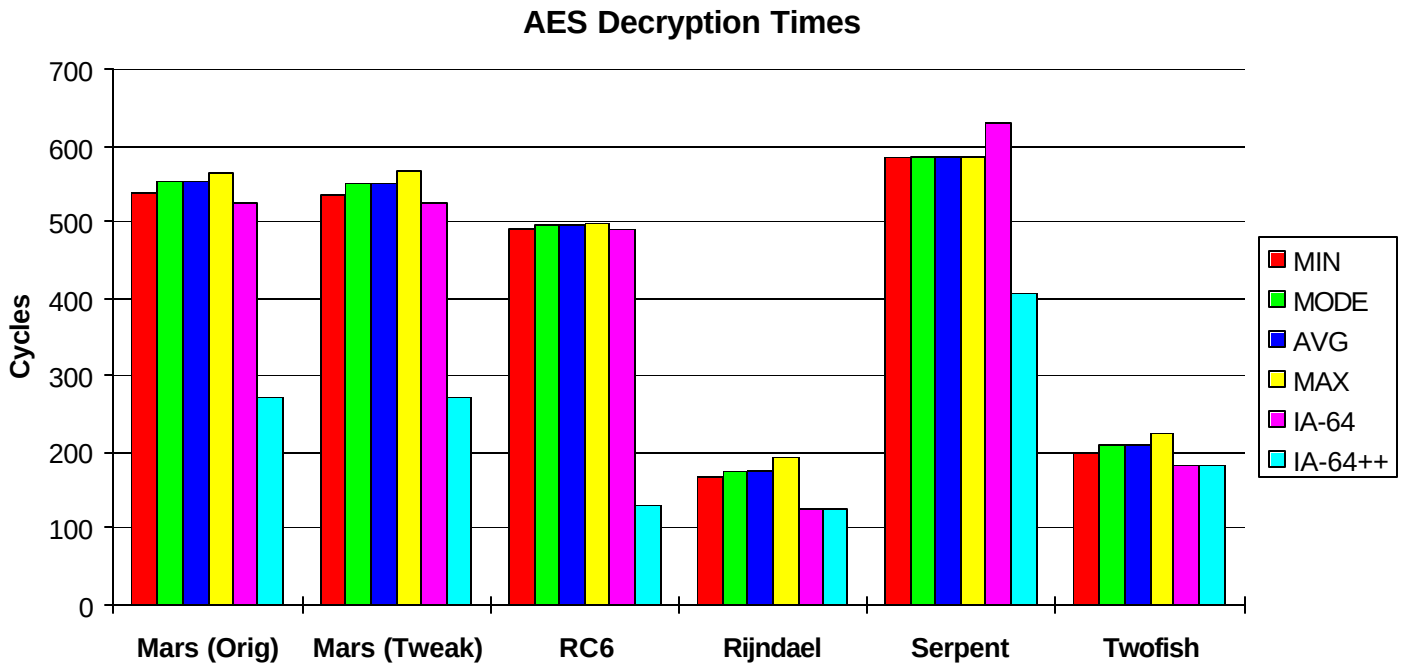
PA-RISC Performance

Decryption Distributions

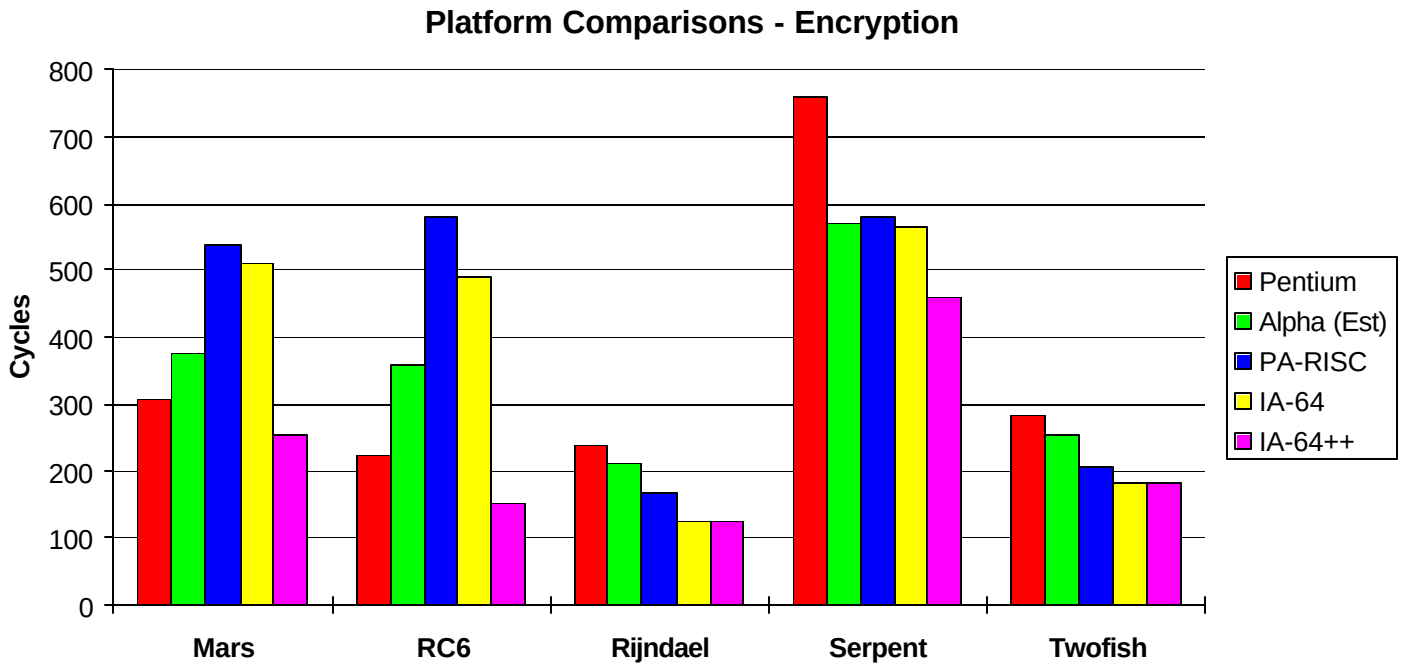
	Min	Avg	Mode	Max	s
Mars	**537**	**551.39**	**552**	**567**	**2.98**
RC6	**493**	**496.37**	**496**	**499**	**0.68**
Rijndael	**168**	**175.88**	**174**	**192**	**2.64**
Serpent	**585**	**586.62**	**587**	**587**	**0.79**
Twofish	**200**	**210.29**	**210**	**224**	**2.48**

Time in cycles

PA-RISC Performance



PA-RISC Performance



IA-64 Performance

- **Performance based on a snapshot of the McKinley design**
- **Development using functional simulators**
- **Final timings using actual chip definition on RTL simulator**

	Mars	RC6	Rijndael	Serpent	Twofish
Keying	**1408**	**1057**	**148**	**475**	**2445**
Encryption	**511**	**490**	**125**	**565**	**182**
Decryption	**527**	**490**	**126**	**631**	**182**

Time in cycles

IA-64++ Performance

Hypothetical IA-64 implementation with…

- **Unsigned 32x32 ® 32 multiplication**
- **32-bit fixed rotation**
- **32-bit variable rotation**

	Mars	RC6	Rijndael	Serpent	Twofish
Keying	**1408**	**1057**	**148**	**380 (475)**	**2445**
Encryption	**255 (511)**	**150 (490)**	**125**	**460 (565)**	**182**
Decryption	**271 (527)**	**130 (490)**	**126**	**407 (631)**	**182**

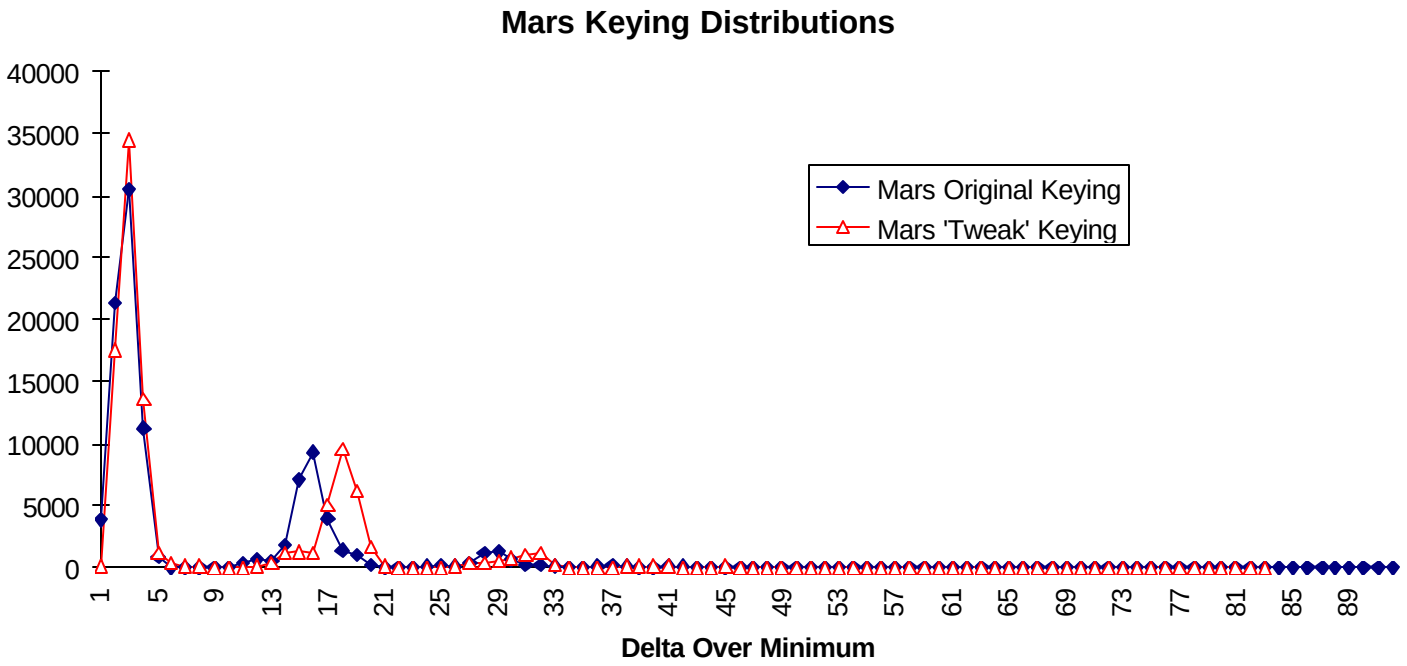
Time in cycles: new (old)

Conclusions

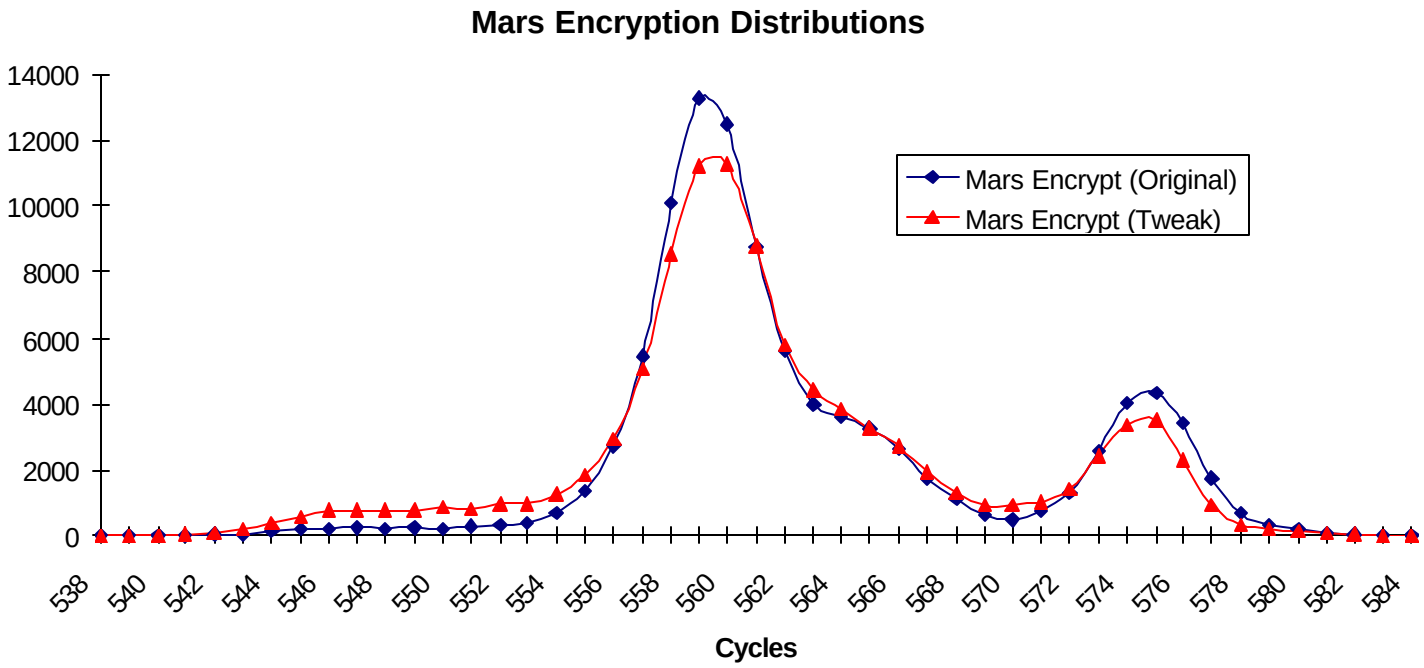
- **All finalists have reasonable implementations on both PA-RISC and IA-64**
- **Software performance is *not* a single number**
- **Algorithm parallelism is an important criterion for future systems**

Performance	**Memory**	**Parallelism**
Rijndael	RC6	Rijndael
RC6 / Twofish	Serpent	Twofish
Twofish / RC6	Mars	Serpent
Mars	Twofish	Mars
Serpent	Rijndael	RC6

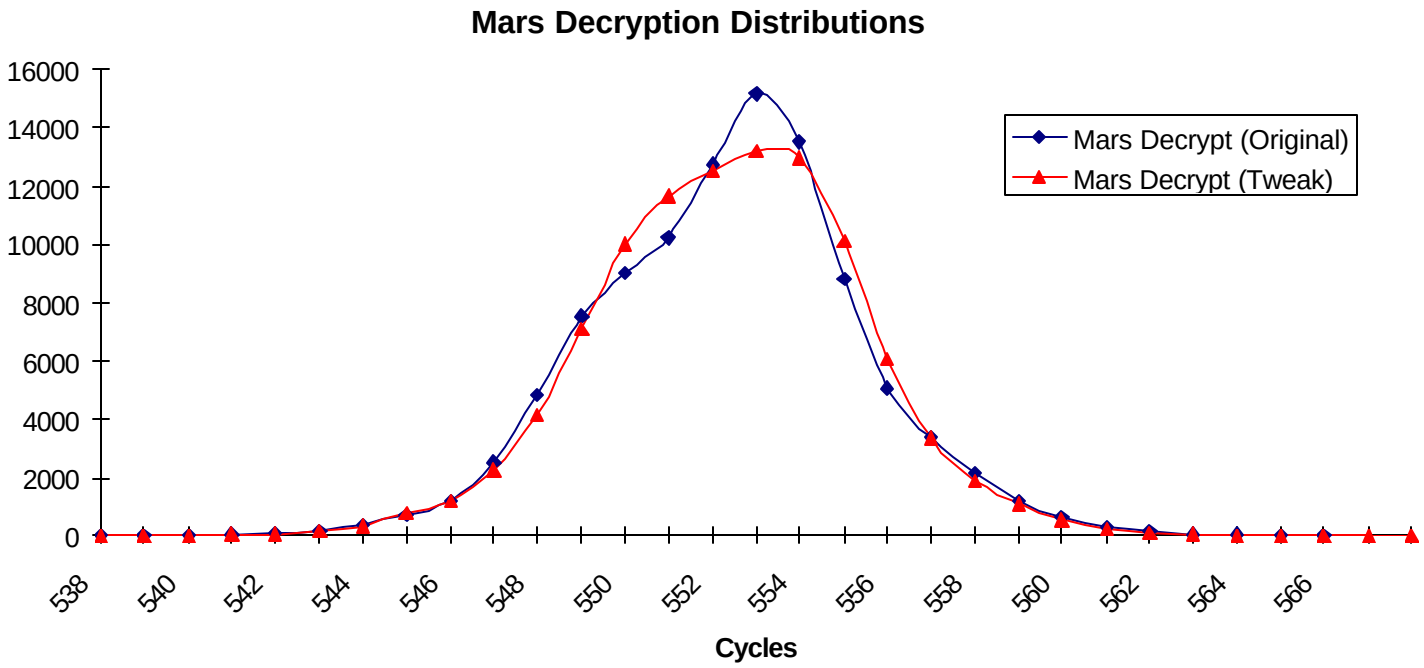
PA-RISC Performance



PA-RISC Performance

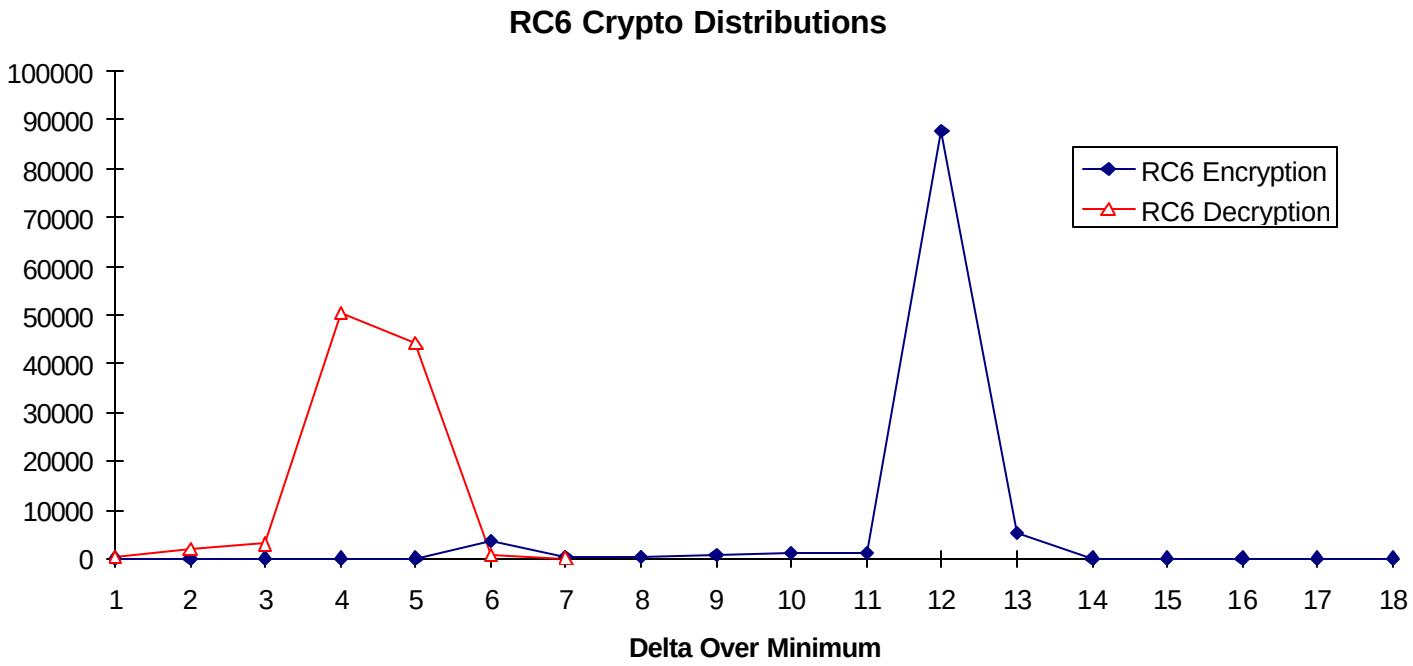


PA-RISC Performance



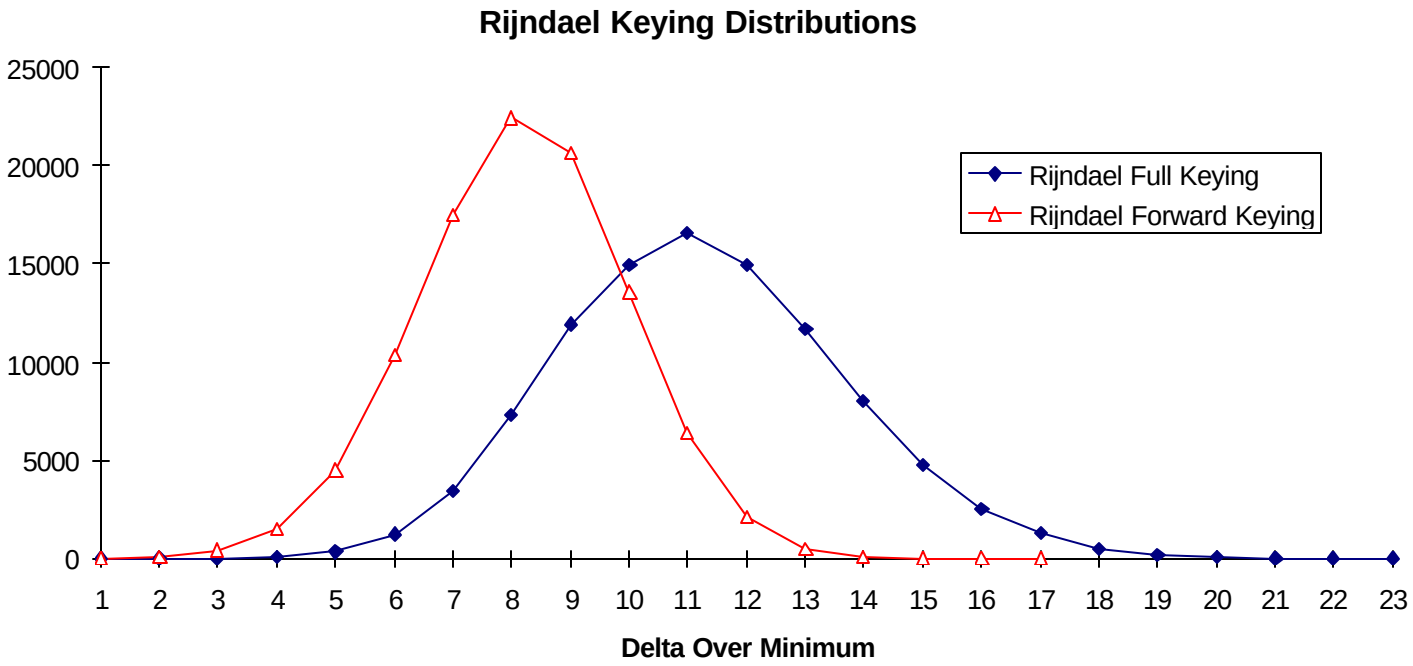
AES

PA-RISC Performance



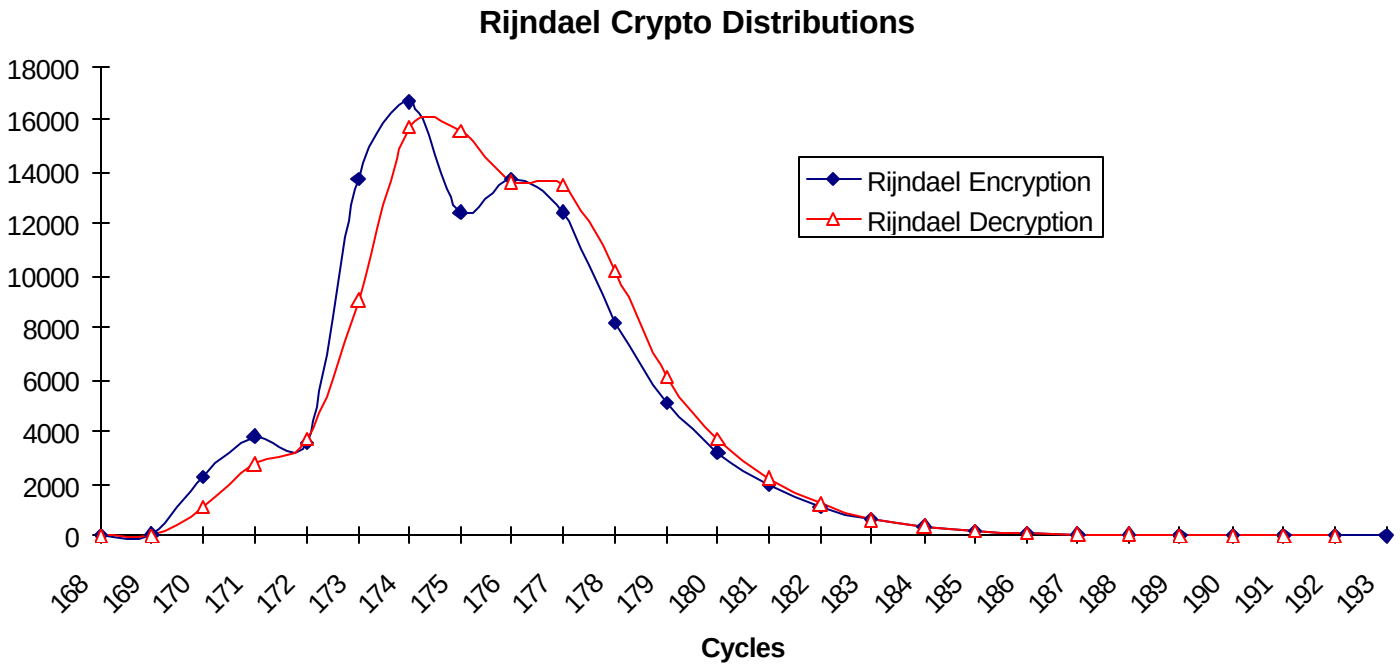
AES

PA-RISC Performance



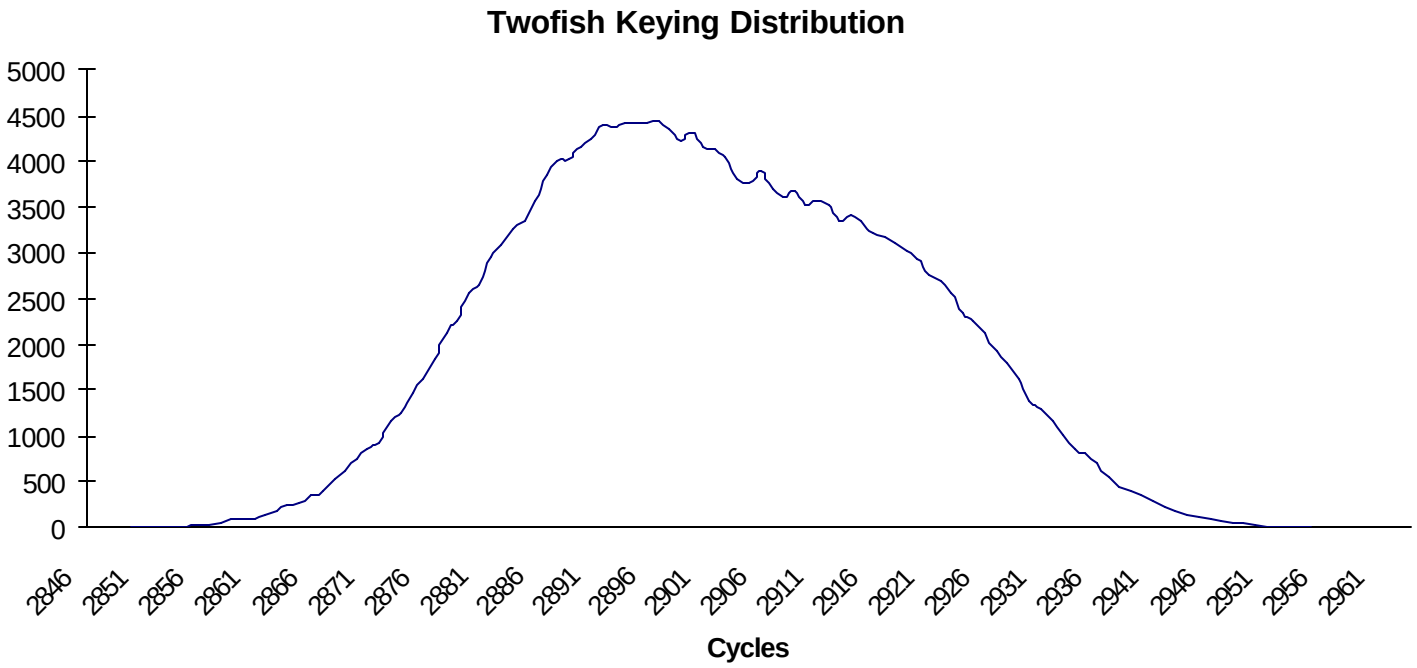
AES

PA-RISC Performance



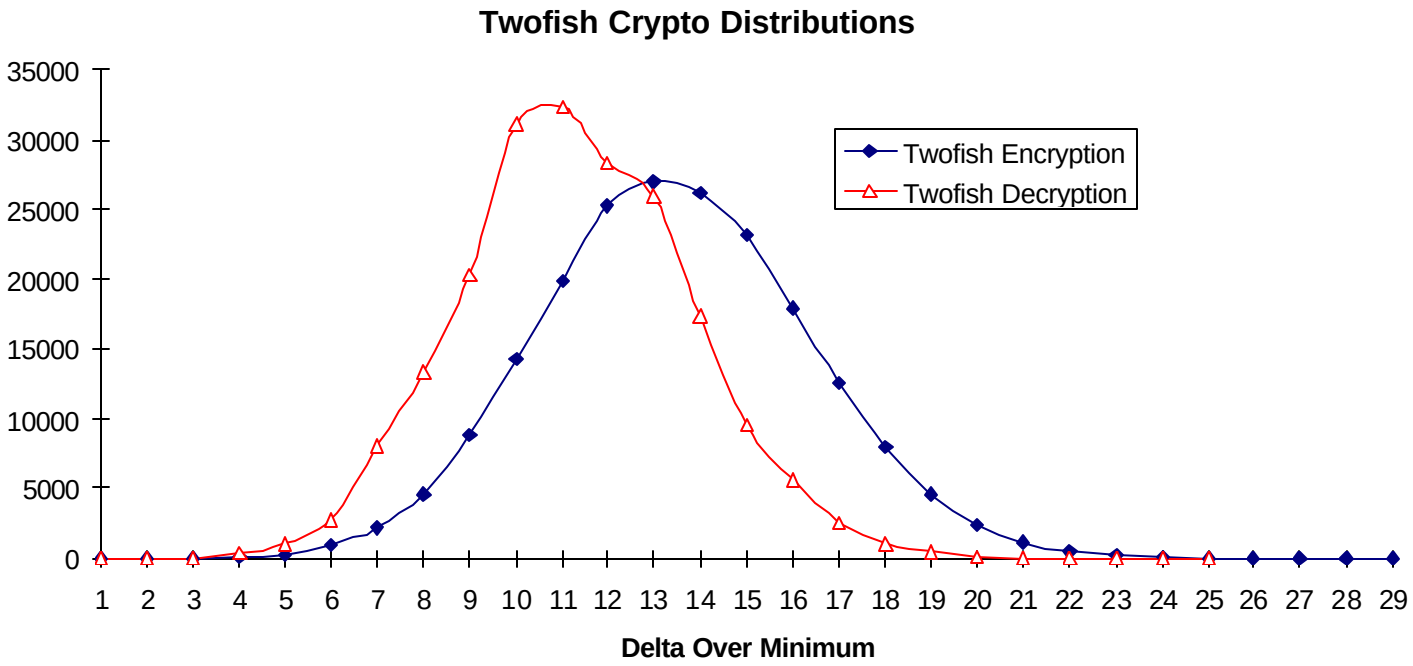
AES

PA-RISC Performance



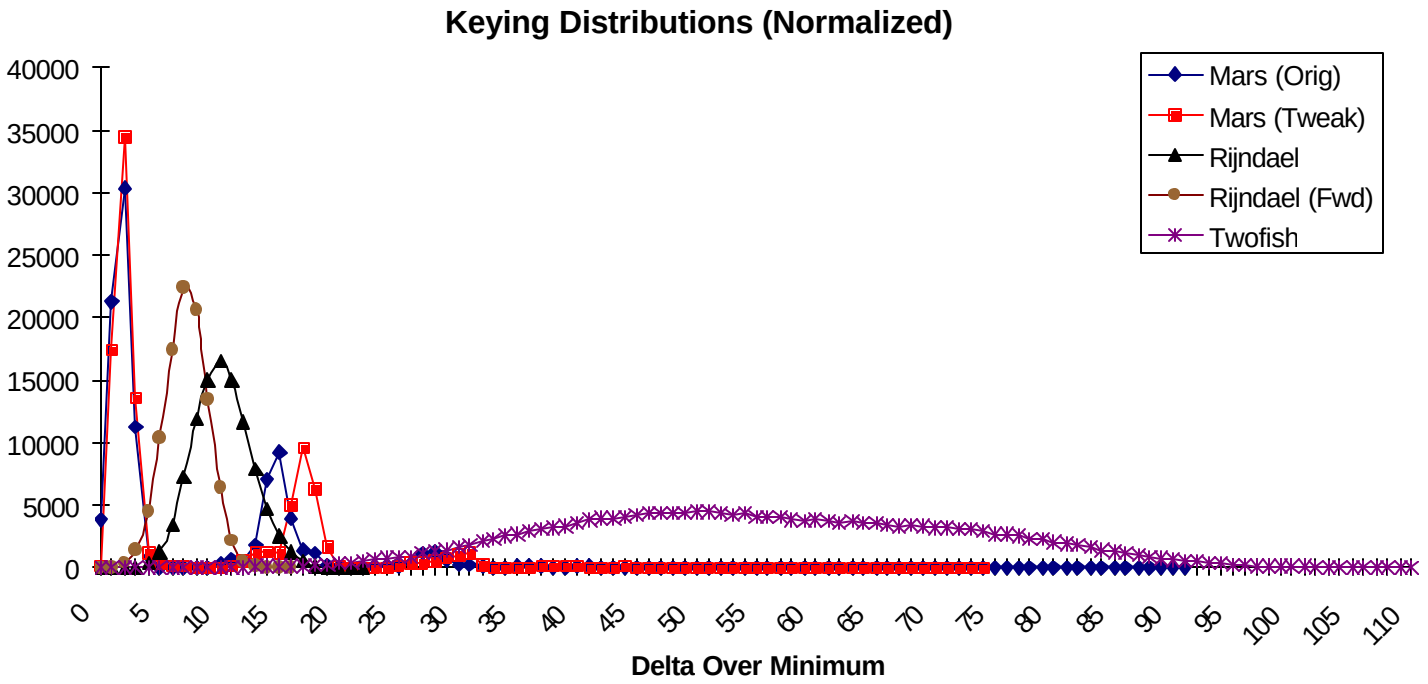
AES

PA-RISC Performance



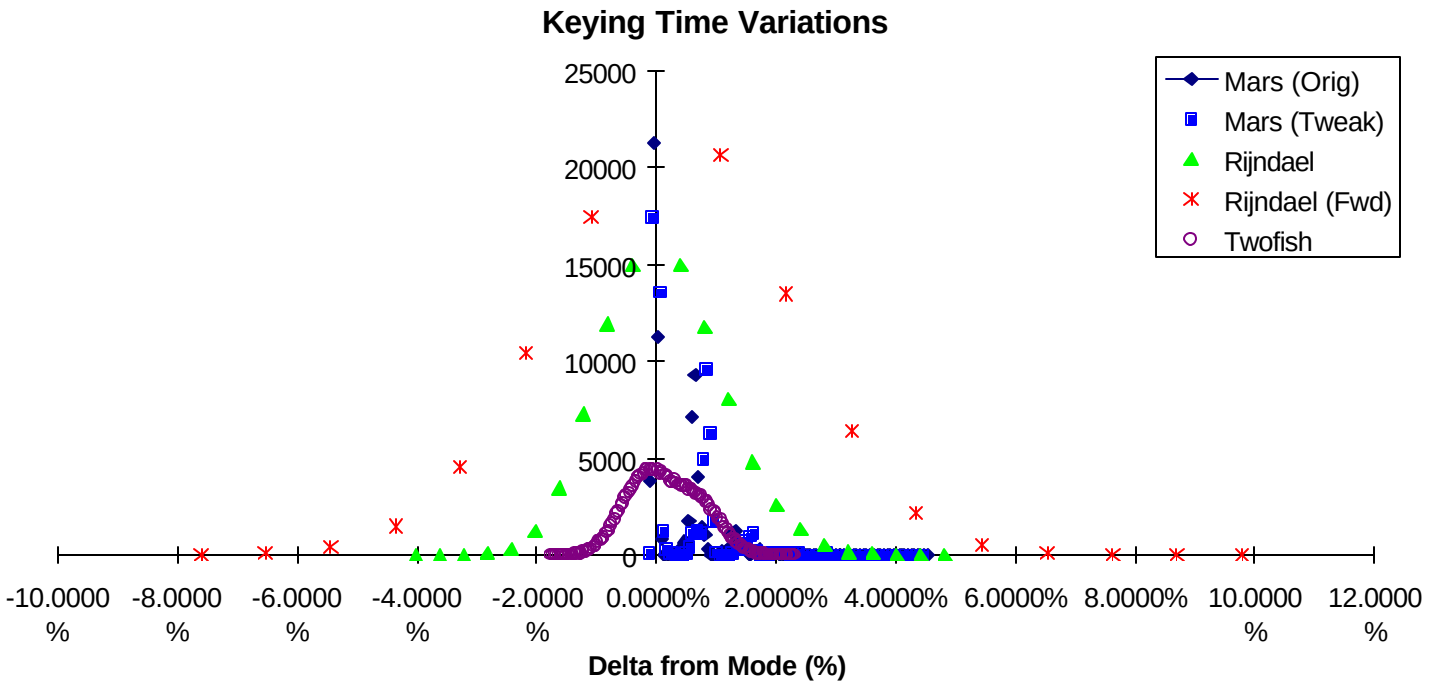
AES

PA-RISC Performance



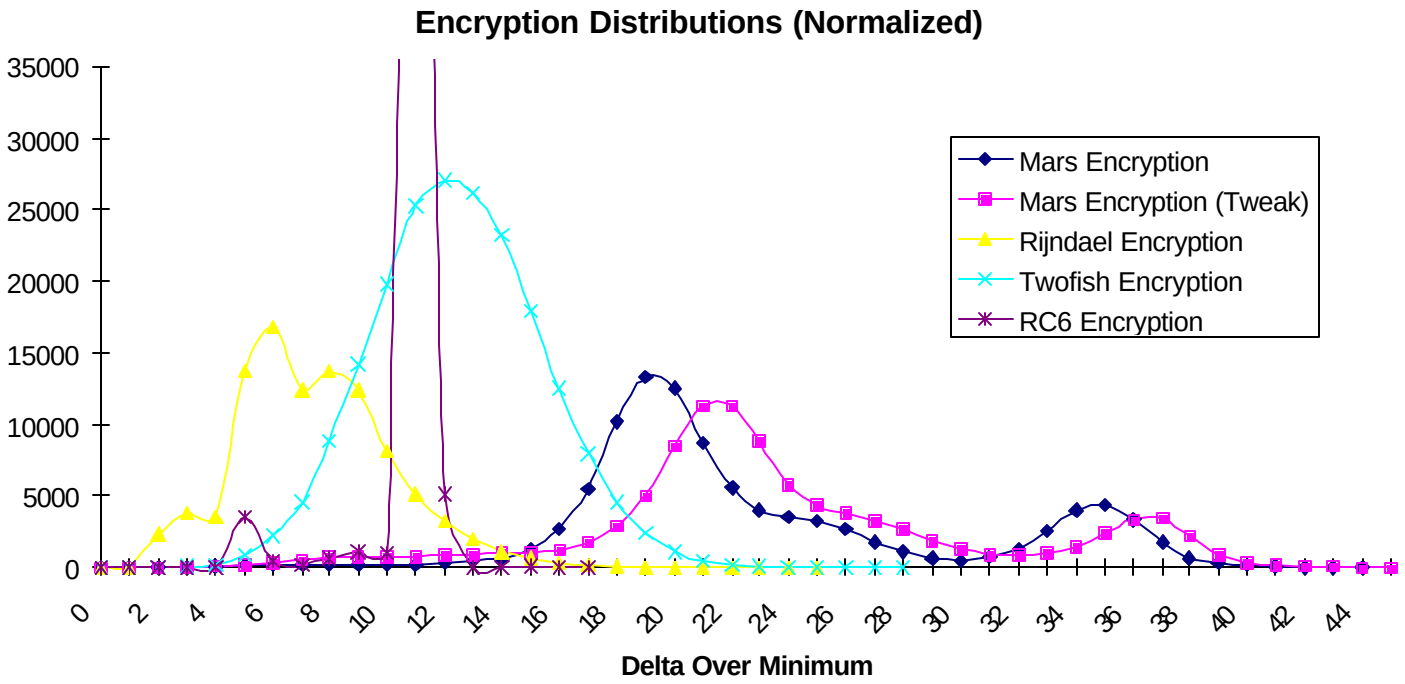
AES

PA-RISC Performance



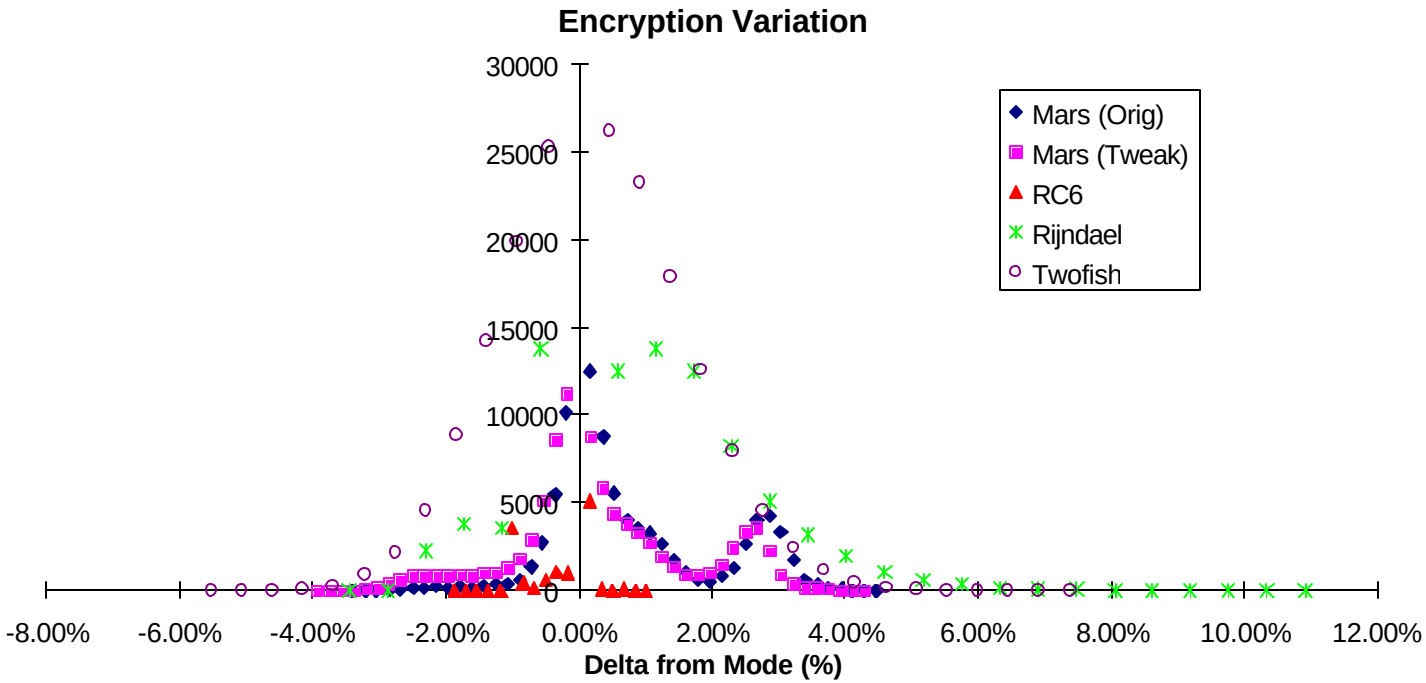
AES

PA-RISC Performance



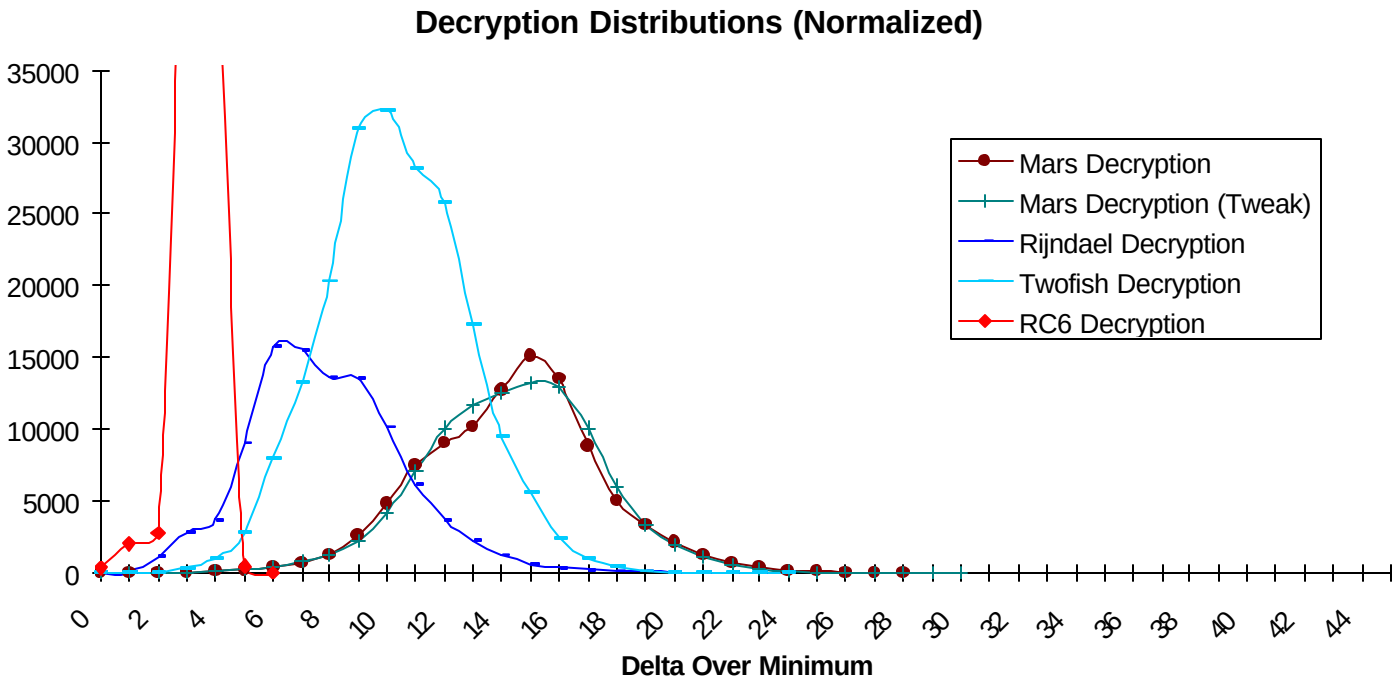
AES

PA-RISC Performance



AES

PA-RISC Performance



AES

PA-RISC Performance