AES Java(TM) Technology Comparisons

Alan Folmsbee
Sun Microsystems, Inc.

Agenda

- The Fractional Feistel Dimension
- Nearly-Ideal Avalanche
- Excess Avalanche Metrics
- Speed Comparisons
- Memory Comparisons
- Conclusions

The Fractional Feistel Dimension "Fracstel"

$$F = \frac{rp}{p - c}$$

r = rounds in avalanche test

p = number of plaintexts

c = number of ciphertexts with no avalanche

Example Fracstel Calculation

$$F = \frac{rp}{p - c} \text{ (units of rounds)}$$

F describes the number of rounds needed so each plaintext bit causes avalanche.

For Twofish, F is an integer:

$$F = \frac{1 * 12800}{12800 - 6400} = (2 \text{ rounds})$$

Discussion of the Fracstel

Candidates have Integer Feistel Dimensions and Fractional Feistel Dimensions:

RC6:

$$F = \frac{1 * 12800}{12800 - 3280} = 1.34 \text{ rounds}$$

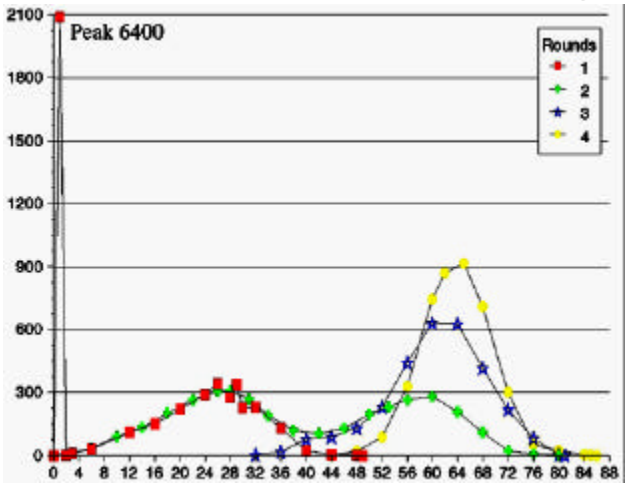
HPC:

$$F = \frac{0.1 * 12800}{12800 - 6145} = 0.19 \text{ rounds}$$

"Nearly-Ideal" Avalanche Round

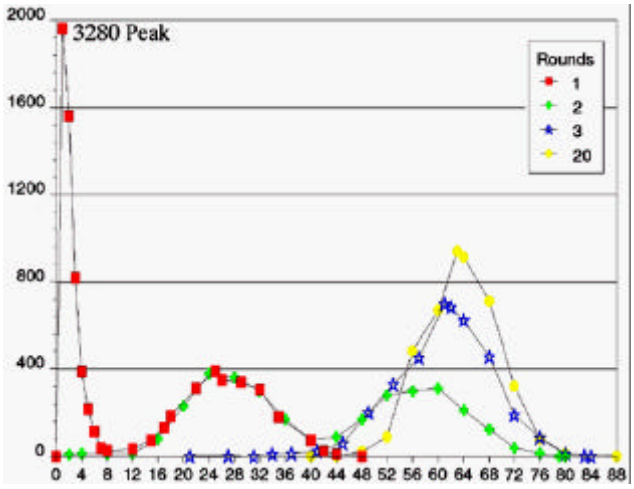
Find the earliest round where avalanche is nearly-ideal

Loki97

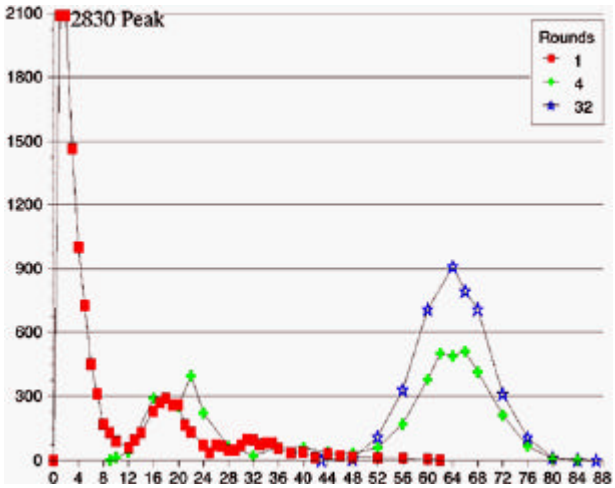


Histogram of avalanche for 12800 encryptions

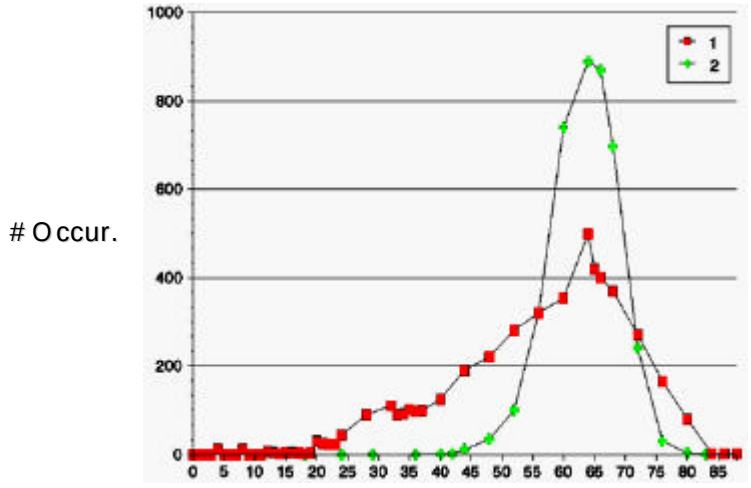
RC6 Avalanche Histogram for 1, 2, 3 and 20 Rounds



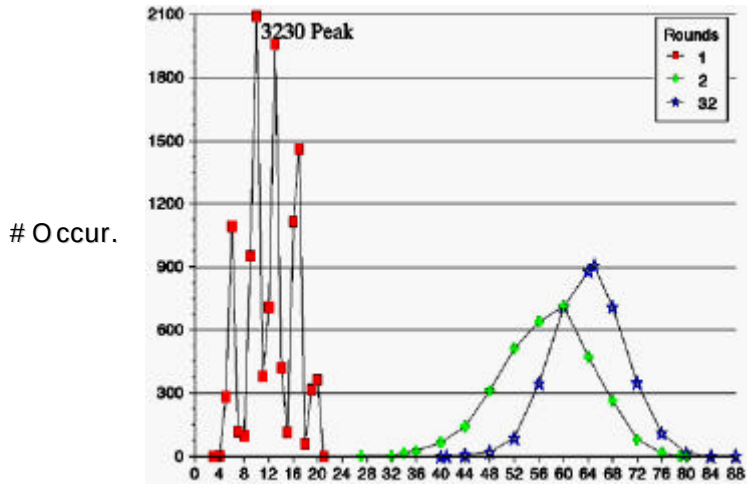
MARS Avalanche for 1, 4 and 32 Rounds



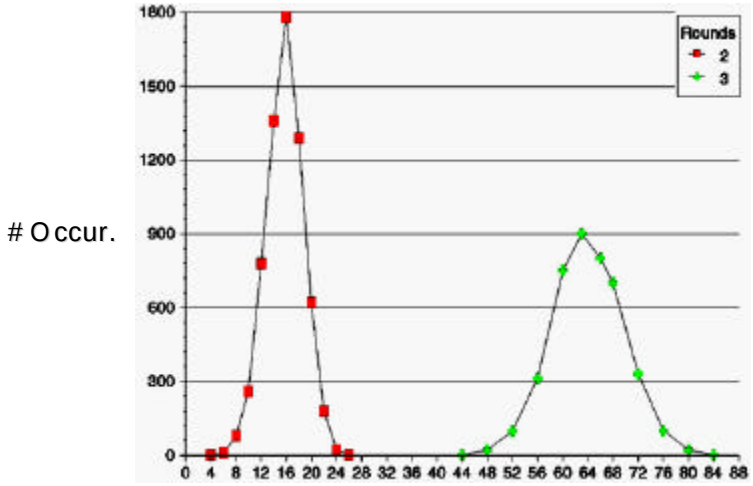
Safer+ Avalanche for Rounds 1 and 2



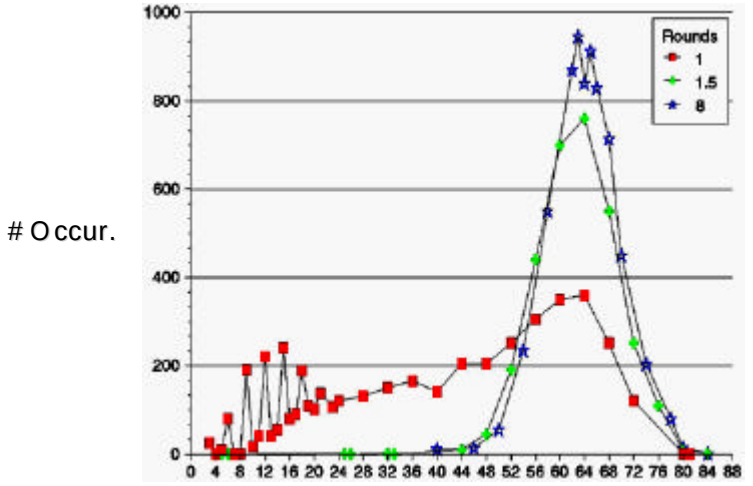
Serpent Avalanche for 1, 2 and 32 Rounds



Crypton Avalanche for 2 and 3 Rounds

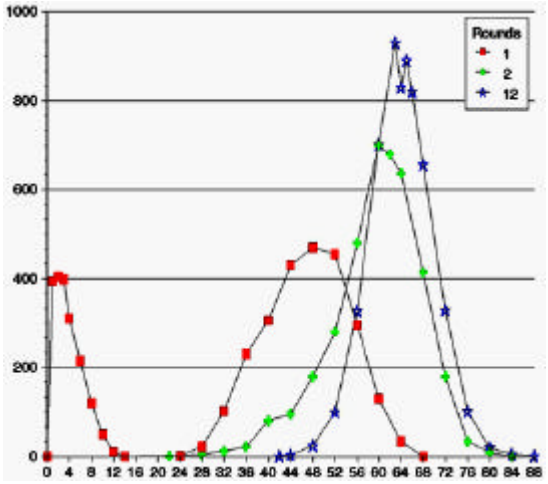


Frog Avalanche for 1, 1.5 and 8 Rounds



E2 Avalanche for 1, 2 and 12 Rounds

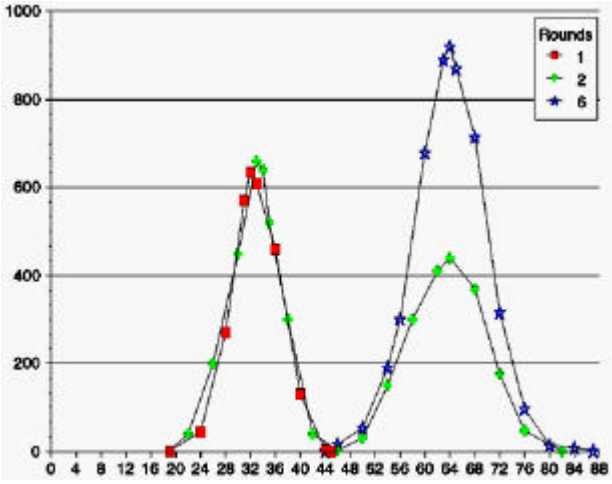
Occur.



Number of Bits that Changed

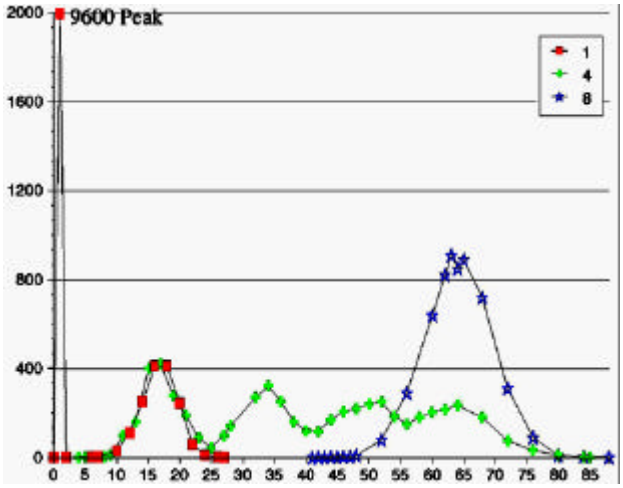
Magenta Avalanche for 1, 2 and 6 Rounds

Occur.



Number of Bits that Changed

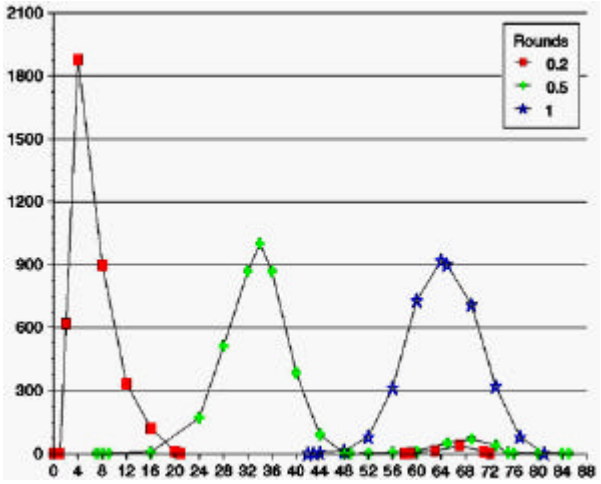
Cast Avalanche for 1, 4 and 8 Rounds



Occur.

Number of Bits that Changed

HPC Avalanche for 0.2, 0.5 and 1 Round

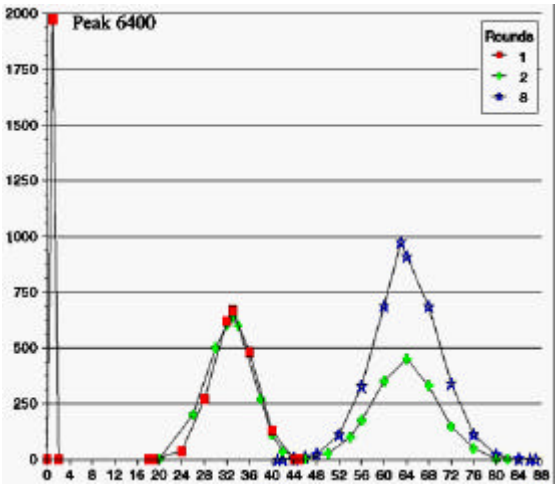


Occur.

Number of Bits that Changed

DFC Avalanche for 1, 2 and 8 Rounds

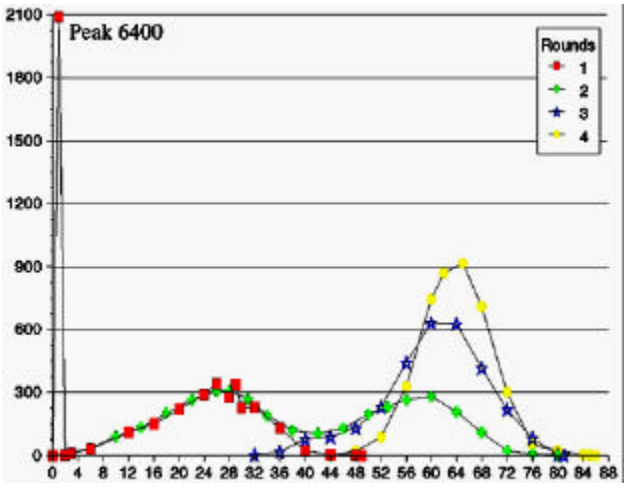
Occur.



Number of Bits that Changed

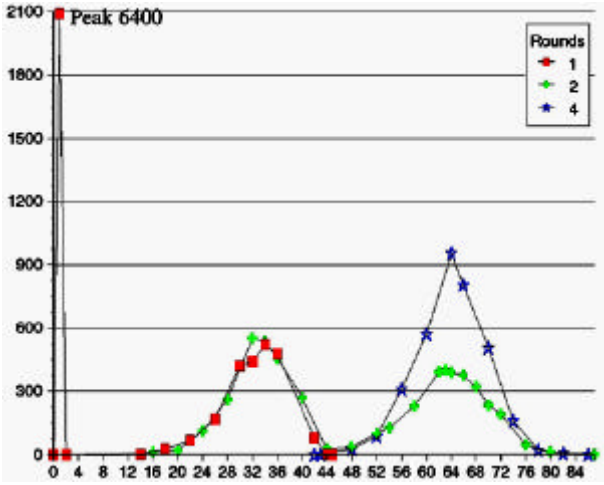
Loki97 Avalanche for 1, 2, 3 and 4 Rounds

Occur.

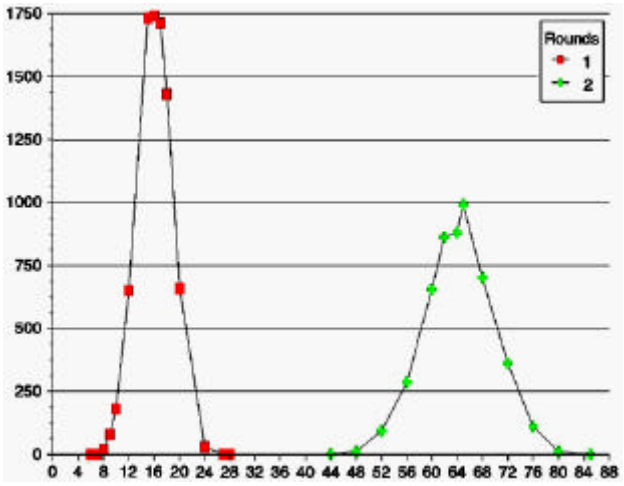


Number of Bits that Changed

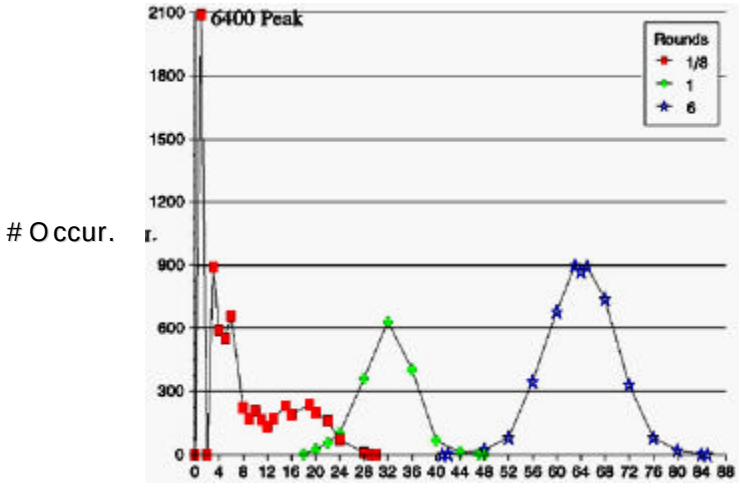
Twofish Avalanche for 1, 2 and 4 Rounds



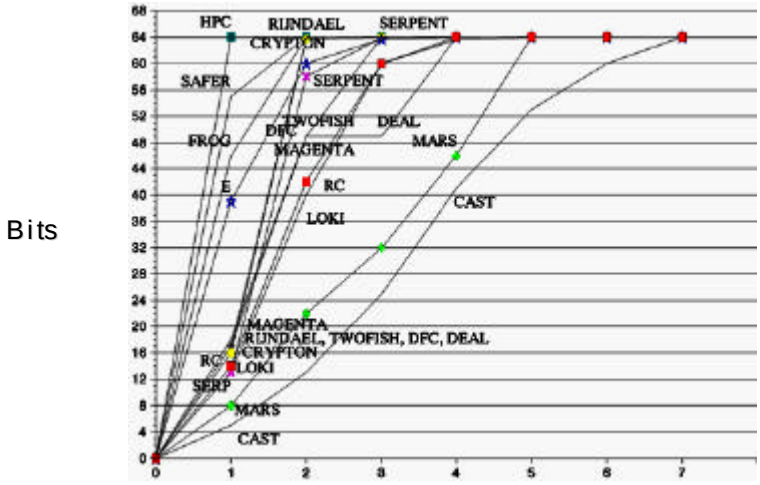
Rijndael Avalanche for 1 and 2 Rounds



DEAL Avalanche for 1/8, 1 and 6 Rounds



Average Avalanche



Avalanche Comparisons

Candidate	Total Rounds	Nearly-Ideal Round	Avalanche Ratio Beyond Nearly-Ideal	Fracstel (rounds)	Excess Fracstel Ratio
SERPENT	32	2	16.0	1.00	32.0
HPC	8	1	8.0	0.19	42.1
RC6	20	3	6.6	1.34	14.9
MARS	32	5	6.4	1.28	25.0
CAST256	48	8	6.0	4.00	12.0
E2	12	2	6.0	1.03	11.6
FROG	8	1.5	5.3	1.00	8.0
LOKI97	16	3	5.3	2.00	8.0
TWOFISH	16	3	5.3	2.00	8.0
RIJNDAEL	10	2	5.0	1.00	10.0
CRYPTON	14	3	4.6	1.00	14.0
SAFER+	8	2	4.0	1.00	8.0
DFC	8	3	2.6	2.00	4.0
MAGENTA	6	3	2.0	2.00	3.0
DEAL	6	4	1.5	2.00	3.0

Two Excess Avalanche Metrics

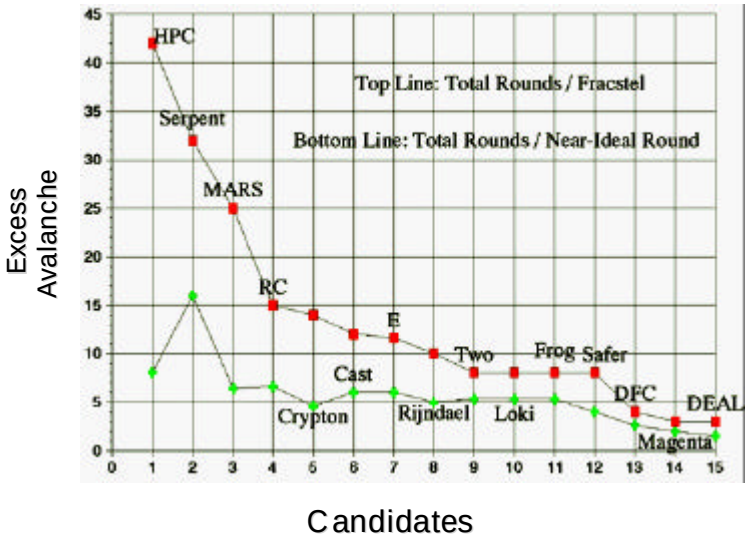


Table of Speed Comparisons

Name	UltraSparc 200 Mhz Encrypt Java Application	UltraSparc MCT Java Application	UltraSparc KAT Java Application
MARS	8400 kilobit/s	3284 kilobit/s	270 kilobit/s
RC6	7840	5061	355
E2	6500	2934	265
SERPENT	4300	2544	238
HPC	4100	2710	185
CRYPTON	4000	2710	281
CAST256	2000	1213	214
TWOFISH	1400	1729	156
FROG	1150	1029	7
SAFER+	790	811	169
DEAL	660	664	176
RIJNDAEL	520	513	184
LOKI97	410	420	161
MAGENTA	150	164	106
DFC	33	35	16

Java CPU Speed vs. Java Virtual Machine

Cryptographic Algorithm	MicroJava 701 100Mhz clock	UltraSparc 200 Mhz clock
MARS	4142 kbits/second	8005 kbits/second
RC6	2300	4880
E2	1641	6700
SERPENT	513	3900
HPC	920	3000
CRYPTON	1094	2500
CAST256	782	1760
TWOFISH	724	1440
FROG	563	1130
SAFER+	329	770
DEAL	142	590
RIJNDAEL	74	420
LOKI97	74	380
MAGENTA	25	140
DFC	8	28

Table of Memory Comparisons

Name	RAM size bytes	ROM size bytes
SAFER+	320	13200
MARS	456	19719
MAGENTA	464	6088
RC6	480	7800
FROG	576	14100
DFC	632	11147
CRYPTON	800	13979
E2	880	275857
SERPENT	1248	38900
CAST256	2260	29000
DEAL	4355	20043
TWOFISH	8000	19181
LOKI97	10240	15956
HPC	15000	44889
RIJNDAEL	20000	18405

Concluding Recommendations

- The top five candidates are:
  - RC6
  - Mars
  - Serpent
  - Hasty Pudding Cipher
  - Crypton
- This conclusion used weights of:
  - 4 for Excess Fracstel Ratio
  - 1 for RAM
  - 1 for ROM
  - 1 for Encryption Speed