Rijndael for AES

Joan Daemen
Proton World

Vincent Rijmen
COSIC

Security

- Intrinsic security: no algorithm has been broken
- Implementation attacks (e.g., DPA):
  - Table-lookup and XOR operations only
  - → Rijndael lends itself to secure implementations on smart cards

Relative efficiency

"Equivalent number of Rijndael rounds"

	# blocks	MARS	RC6	Serpent	Twofish
Pentium	Many	13	9	38	12
	4	28	15	33	27
	1	46	22	36	25
6805	Many	30	28	110	23
	4	52	45	107	23
	1	114	91	100	22

Design Philosophy

- Simplicity
- Symmetry
- Parallelism
- Mutual independence of components
  - impact of replacing a component on security analysis is limited
- Rijndael is easily extendible
  - block length, key length, number of rounds

Speed on *unknown platforms*

- "Unknown platforms":
  - parallel processors,
  - vulnerable platforms,
  - high key agility
- No arithmetical operations
- No data-dependent rotations
- Light key schedule

Conclusions

In the many surveys, Rijndael comes out

- sometimes ahead of the pack
- often among the best
- NEVER problematic

VERSATILITY makes Rijndael best candidate