TWOFISH:
New Results

Bruce Schneier, Counterpane Systems
John Kelsey, Counterpane Systems
Doug Whiting, Hi/fn
David Wagner, UC Berkeley
Chris Hall, Counterpane Systems
Niels Ferguson, Counterpane Systems

http://www.counterpane.com/twofish.html

COUNTERPANE SYSTEMS

Three Parts

- Improved Twofish Implementations
- Empirical Verification of Twofish Key Uniqueness Properties
- Upper Bounds on Differential Characteristics in Twofish

- This talk will concentrate on the first part.

COUNTERPANE SYSTEMS

hi/fn

Improved Assembly Language Performance

- The fastest assembly-language implementations have been sped up.
- These implementations are "compiled mode"; very PentiumPro/II specific..

COUNTERPANE SYSTEMS

hi/fn

Assembly Speed for Different Key Lengths

Processor	Lang	Keying Option	Code Size	Clocks to Key			Clocks to Encrypt		
				128	192	256	128	192	256
PPro/II	ASM	Comp.	9000	8600	11300	14100	258	258	258
PPro/II	ASM	Full	8500	7600	10400	13200	315	315	315
Ppro/II	ASM	Part	10700	4900	7600	10500	460	460	460
PPro/II	ASM	Min.	13600	2400	5300	8200	720	720	720
PPro/II	ASM	Zero	9100	1250	1600	2000	860	1130	1420
Pentium	ASM	Comp.	9100	12300	14600	17100	290	290	290
Pentium	ASM	Full	8200	1000	13500	16200	315	315	315
Pentium	ASM	Part	10300	5500	7800	9800	430	430	430
Pentium	ASM	Min.	12600	3700	5900	7900	740	740	740
Pentium	ASM	Zero	8700	1800	2100	2600	1000	1300	1600

Twofish ASM performance with
different key lengths and options

COUNTERPANE SYSTEMS

hi/fn

Large Memory Implementations

- Some of the fastest DES implementations assume large tables, requiring hundreds of kilobytes.
- Twofish can benefit from the same implementation tricks.
- About 256K of RAM is required.
- These implementations encrypt at the same speed, but have faster key setup times.
- An implementation with 256M of RAM is even faster, but this is not realistic.

COUNTERPANE SYSTEMS

hi/fn

Performance with Large Fixed Tables

				Clocks to Key			Clocks to Encrypt		
Processor	Lang	Keying Option	Code Size	128	192	256	128	192	256
PPro/II	ASM	Comp.	271200	6500	9200	11900	285	285	285
PPro/II	ASM	Full	270600	5300	8000	11000	315	315	315
PPro/II	ASM	Part.	272900	2600	5300	8200	460	460	460
PPro/II	MS C	Full	273300	7300	11200	15700	600	600	600

Twofish performance with large fixed tables

COUNTERPANE SYSTEMS

hi/fn

What's the Point?

- Twofish is unique in that it was designed for implementation tradeoffs.
- There are many ways to trade off encryption speed versus key setup speed.
- The large-RAM implementations show that it is also possible to trade off RAM for key-setup speed.
- This kind of flexibility is important, if an algorithm is going to become a standard.

COUNTERPANE SYSTEMS

hi/fn

Smart Card Performance

- Twofish exhibits the same ability to trade off implementation parameters on a smart card:
  - Memory (both working RAM and key storage)
  - Code and table size
  - Execution speed
- Twofish can fit on the smallest of smart cards (24 bytes for the key + 36 bytes working RAM + 2000 bytes for code and tables).
- Twofish can take advantage of more memory by encrypting faster and/or requiring less code.

COUNTERPANE SYSTEMS

hi/fn

6805 Smart Card

RAM, ROM or EEPROM for Key	Working RAM	Code and Table Size	Clocks per Block	Time per Block @ 4MHz
24	36	2200	26500	6.6 msec
24	36	2150	32900	8.2 msec
24	36	2000	35000	8.7 msec
24	36	1750	37100	9.3 msec
184	36	1900	15300	3.8 msec
184	36	1700	18100	4.5 msec
184	36	1450	19200	4.8 msec
1208	36	1300	12700	3.2 msec
1208	36	1100	15500	3.9 msec
1208	36	850	16600	4.2 msec
3256	36	1000	11900	3.0 msec

Twofish performance, with a 128-bit key,
on a 6805 smart card

COUNTERPANE SYSTEMS hi/fn

Hardware Performance

- Twofish's implementation flexibility is also evident in hardware implementations.
- The same tradeoffs are possible.
- The new line in this table is an 8000-gate implementation.
- Other hardware implementations are possible.

COUNTERPANE SYSTEMS hi/fn

Hardware Tradeoffs

Gate Count	*h* Blocks	Clocks/ Block	Interleave Levels	Clock Speed	Throughput (Mbits/sec)	Startup Clocks
8000	0.25	324	1	80 MHz	32	20
14000	1	72	1	40 MHz	71	4
19000	1	32	1	40 MHz	160	40
123000	2	16	1	40 MHz	320	20
26000	2	32	2	80 MHz	640	20
28000	2	48	3	120 MHz	960	20
30000	2	64	4	140 MHz	1200	20
80000	2	16	1	80 MHz	640	300

Hardware tradeoffs (128-bit key)

COUNTERPANE SYSTEMS hi/fn

Part 2: Verification of Key Uniqueness Properties

- We looked at the Twofish key schedule in an attempt to prove various things about it.
- This is especially important in related-key attacks, and if the algorithm is being used as a hash function.

COUNTERPANE SYSTEMS hi/fn

What we Proved

- No two distinct keys produce an identical sequence of subkeys.
- Each distinct value for S results in a unique round function, f.
- Empirical verification techniques

COUNTERPANE SYSTEMS

hi/fn

Part 3: Upper Bound on Differential Characteristics

- To learn more about differential attacks on Twofish we tried to derive a strict upper bound on the probability of a Twofish differential characteristic.

COUNTERPANE SYSTEMS

hi/fn

Method Used

- Classify 1-round differentials into different categories.
- Compute an upper bound on the probabilities of the differentials in each category.
- Piece together the categories into multi-round characteristics.

COUNTERPANE SYSTEMS hi/fn

Result

- Any 12-round differential characteristic has a probability of at most $2^{-102.8}$
- Bound is not quite strict, but it is very conservative.
- We expect further improvements on this bound by using sharper bounds on various components.

COUNTERPANE SYSTEMS hi/fn

Differential Probabilities

	128-bit key	192-bit key	256-bit key
Sbox 0	$1.0649 \cdot 2^{-8}$	$1.0084 \cdot 2^{-8}$	$1.0043 \cdot 2^{-8}$
Sbox 1	$1.0566 \cdot 2^{-8}$	$1.0087 \cdot 2^{-8}$	$1.0043 \cdot 2^{-8}$
Sbox 2	$1.0533 \cdot 2^{-8}$	$1.0097 \cdot 2^{-8}$	$1.0045 \cdot 2^{-8}$
Sbox 3	$1.0538 \cdot 2^{-8}$	$1.0088 \cdot 2^{-8}$	$1.0044 \cdot 2^{-8}$

COUNTERPANE SYSTEMS

hi/fn