

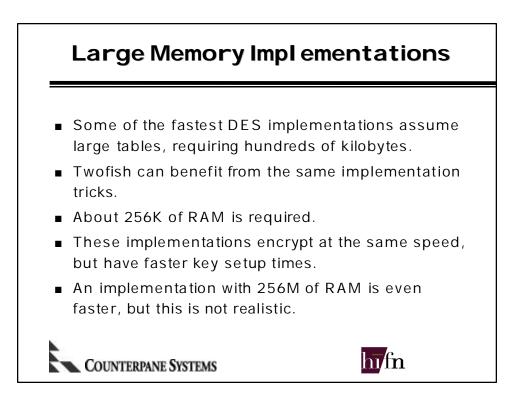
Assembly Speed for Different Key Lengths

		Keying		Cl	ocks to K	ley	Cloc	cks to En	crypt
Processor	Lang	Option	Code Size	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







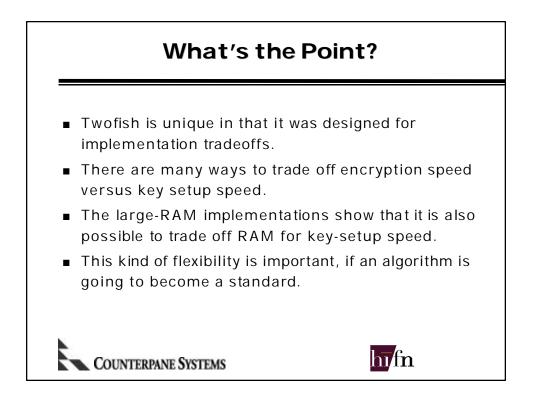
Performance with Large Fixed Tables

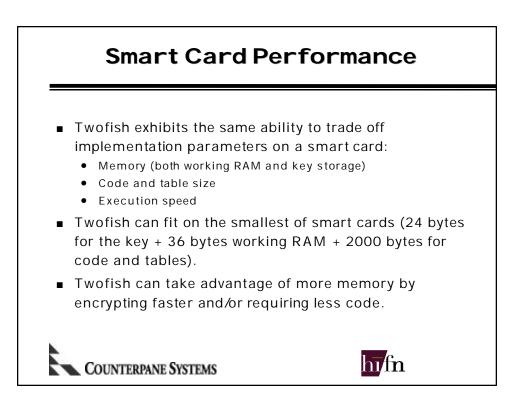
		Keying		C	locks to K	ey	Clocks to Encryp		crypt
Processor	Lang	Option	Code Size	128	192	256	128	192	256
PPro/II	ASM	Comp.	271200	6500	9200	11900	285	285	285
PPro/II	ASM	Full	270600	5300	8000	11000	315	315	315
PPro/II	ASM	Part.	272900	2600	5300	8200	460	460	460
PPro/II	MS C	Full	273300	7300	11200	15700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

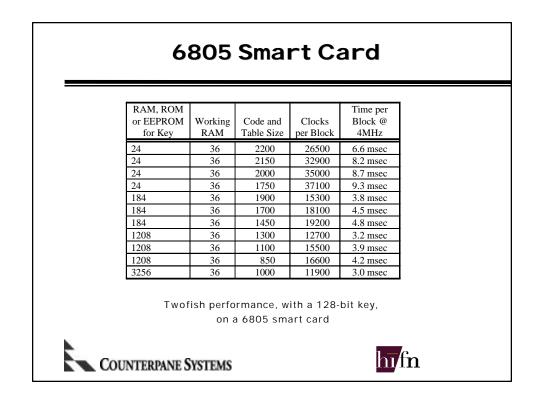
Twofish performance with large fixed tables

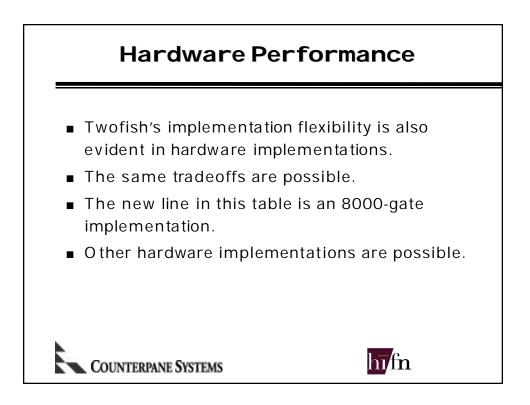
COUNTERPANE SYSTEMS

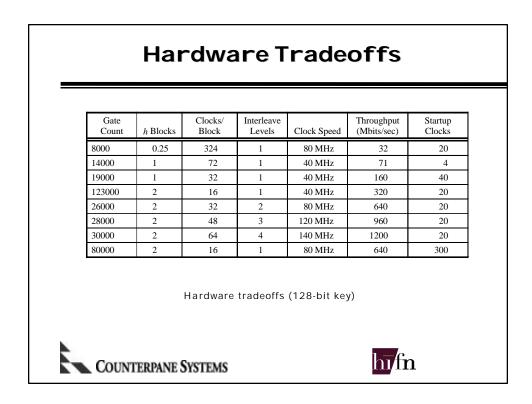


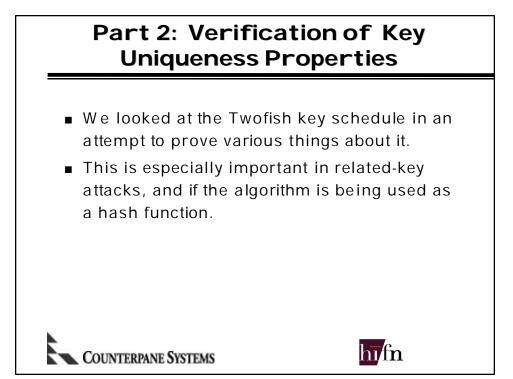


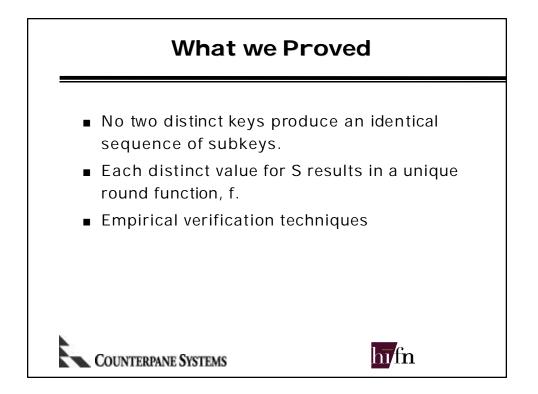










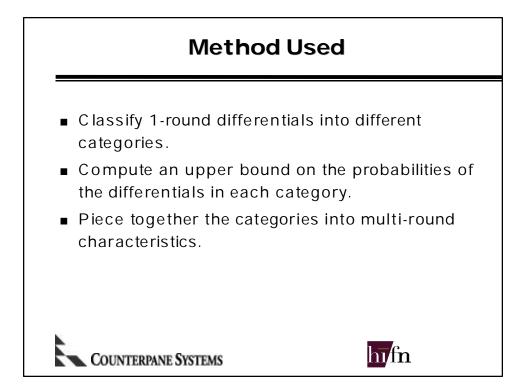


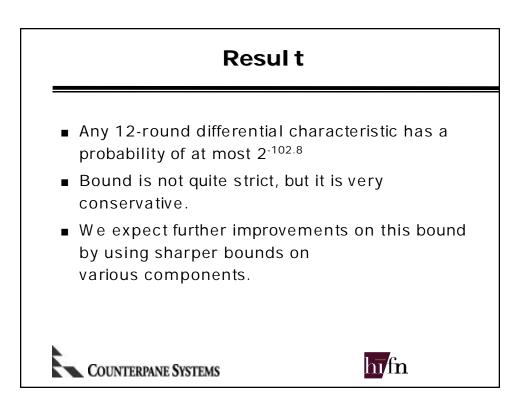
Part 3: Upper Bound on Differential Characteristics

 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







	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	$1.0566\cdot 2^{-8}$	$1.0087\cdot2^{-8}$	$1.0043\cdot2^{-8}$
Sbox 2	$1.0533\cdot2^{-8}$	$1.0097 \cdot 2^{-8}$	$1.0045\cdot2^{-8}$
Sbox 3	$1.0538\cdot2^{-8}$	$1.0088\cdot2^{-8}$	$1.0044\cdot2^{-8}$

COUNTERPANE SYSTEMS

hī/fn