Results on the implementations of Khazad, MISTY1 and SAFER++ on a 8051 cpu

NES/DOC/ENS/WP6/030/2 [*][†]

Emmanuelle Dottax
École Normale Supérieure

September 17, 2002.

The following table summarizes the results for our Khazad, MISTY1 and SAFER++ implementations on a 8-bit smart-card (8051). The RAM and ROM are expressed in bytes. The "(+16)" means that 16 bytes must be added if the key is to be kept. The given number of cycles is for the encryption of a 8-byte block *and* the key schedule.

	RAM	ROM (code + tables)	Cycles
Khazad	41(+16)	1227 (705 + 512)	4000
MISTY1	31(+16)	2682 (1530 + 1152)	5280
SAFER++	35(+16)	1345 (705 + 640)	3966

[*] This work has been supported by the Commission of the European Communities through the IST Program under Contract IST-1999-12324 (NESSIE).

[†] The information in this document is provided as is, and no warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information as its sole risk and liability.