Performance Benchmarking

Execution Time

Implementation	Time [ms]
Reference Card	4.95
Own implementation (no countermeasure)	2.02
Own implementation + Dummy Operations	6.83
Own implementation + Shuffling	7.85
Own implementation + Masking	5.95
Own implementation + Masking + Shuffling	11.85

Memory

Implementation	Program [KB]	Data [KB]
Own implementation (no countermeasure)	11.81	0.46
Own implementation + Dummy Operations	13.13	0.50
Own implementation + Shuffling	14.02	0.52
Own implementation + Masking	14.21	1.30
Own implementation + Masking + Shuffling	17.06	1.34

DPA Attack

Implementation	Broken?	No. of Traces	Time [s]
Own implementation (no countermeasure)	Yes	400	1.7241
Own implementation + Dummy Operations	Yes	1000	15.3426
Own implementation + Shuffling	Yes	4000	71.5412
Own implementation + Masking	No	6000	
Own implementation + Masking + Shuffling	No	10000	