OBSAH

1 ÚVOD 5

2 PŘEHLED SOUČASNÉHO STAVU PROBLEMATIKY 6

2.1 Útok výkonovým postranním kanálem 6
2.2 Korelace průběhů výkonové spotřeby s operacemi A operandy zpracovávanými šifrovacím Algoritmem 8

3 CÍLE DIZERTAČNÍ PRÁCE 8

4 JEDNODUCHÁ VÝKONOVÁ ANALÝZA 9

5 DIFERENČNÍ VÝKONOVÁ ANALÝZA 11

5.1 Útok výkonovým postranním kanálem s diferenční analýzou založenou na rozdílu středních hodnot 12
5.2 Praktická realizace útoku za pomocí diferenční výkonové analýzy na šifrovací algoritmus DES 13
5.2.1 Znalost otevřeného textu 14
5.2.2 Znalost šifrovaného textu 15

6 EXPERIMENTÁLNÍ PRACOVIŠTĚ PRO SIMULACI ÚTOKŮ VÝKONOVÝM POSTRANNÍM KANÁLEM 15

6.1 Kryptografický modul 16
6.2 Programové vybavení pro diferenční výkonovou analýzu 17
6.3 Měření výkonových průběhů 19

7 NAPÁJECÍ SYSTÉM KRYPTOGRAFICKÉHO MODULU 19

7.1 Rozvod napájení v elektronickém zařízení 20
7.1.1 Úsek mezi napájecím zdrojem a funkčními bloky 21
7.1.2 Úsek v rámci bloku 21
7.2 Blokovací kondenzátory 22
7.2.1 Lokální blokovací kondenzátor 23
7.2.2 Skupinový blokovací kondenzátor 23

8 VÝSLEDKY MĚŘENÍ VÝKONOVÝCH PRŮBĚHŮ V KLÍČOVÝCH MÍSTECH NAPÁJECÍHO SYSTÉMU 23

8.1 popis měření 23
8.2 Shrnutí a vyhodnocení získaných výsledků 25

9 ZÁVĚR 26

LITERATURA 28