

OBSAH

| | |
|---|----|
| Úvod | 5 |
| 1 Cíle disertace | 6 |
| 2 Současný stav problematiky | 7 |
| 2.1 Jednoduchá proudová analýza SPA | 7 |
| 2.2 Diferenciální proudová analýza DPA | 7 |
| 2.2.1 Útok založený na korelačním koeficientu | 9 |
| 2.2.2 Útok založený na rozdílu středních hodnot | 9 |
| 2.2.3 Diferenciální proudová analýza - shrnutí | 10 |
| 2.3 Protiopatření proti proudové analýze | 10 |
| 2.4 Neuronové sítě v kryptografii | 11 |
| 3 Vlastní řešení - proudová analýza | 12 |
| 3.1 Proudová analýza využívající neuronové sítě | 12 |
| 4 Závěr | 25 |
| Literatura | 26 |
| Literatura | 28 |