先端科学技術研究科　修士論文要旨

所属研究室 (主指導教員)	情報セキュリティ工学 (林　優一 (教授))		
学籍番号	2111405	提出日	令和 6年 1月 19日
学生氏名	北村　圭輝		
論文題目	伝達特性を考慮した深層学習サイドチャネル解析のモデル移植性に関する研究		

要旨

深層学習サイドチャネル解析(DLSCA)において、計測環境の差異により生ずる秘密鍵の推定精度の低下は移植性の問題として議論されている。本論文では、平均化による計測波形のノイズ除去と攻撃フェーズとプロファイリングフェーズで計測したサイドチャネル波形の伝達特性の差異に着目することで、攻撃フェーズで計測したサイドチャネル波形の概形をプロファイリングフェーズで計測したサイドチャネル波形に近づけることにより、攻撃フェーズにおいて秘密鍵の推定精度の劣化を引き起こす学習モデルの移植性低下の問題を抑制する手法を提案した。