深層強化学習と制約プログラミングを融合したハイブリットソルバーの軽量ブロック暗号解析への応用

Application of a Hybrid Solver Combining Deep Reinforcement Learning and Constraint Programming to Lightweight Block Cryptanalysis

末吉璃子・システム分科会・情報セキュリティ大学院大学

1．先行研究調査結果

- 既存の暗号攻撃 → 差分攻撃
- 差分を求める → SAT.SMTが有効
- 計算時間と状態数を減らすには
  →深層強化学習

2．目標設定

軽量ブロック暗号を対象として深層強化学習と制約プログラミングを用いて差分を求める

3．実験方法

既存のCryptosmtのフレームを活かし、Hybrid-cp-rl-solverを暗号解析向けに改造し、差分を抽出する。

4．対外的な発表目標

- SUMMER SYMPOSIUMCSS　2022
- CSS
- 研究会:数理モデル化と問題解決（MPS）
- SCIS

5．M2での研究方針・マイルストーン