# 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

**Abstract**：In recent years, there has been a lot of research on the application of machine learning in the area of cryptanalysis. At CRYPTO'19, Aron Gohr [1] proved that a neural distinguisher (which guesses the key) has a higher analysis ability than the distinguisher using existing analysis techniques in lightweight block ciphers. Starting from that research, analysis using machine learning, especially deep learning, has become popular. Differential attacks are known to be the most effective in existing attacks, and research has been done on extracting the differences and guessing the key using SAT. However, the existing tools using SAT and SMT take a long time to analyze and the amount of computation becomes exponentially huge. In addition, it becomes difficult to obtain good differences when the weights are high, the rounds are high, and the sizes are 32/64 (large). Furthermore, there are a few studies that use machine learning for cryptanalysis in SAT and SMT. In this study, we focus on hybrid-cp-rl-solver[2], a tool for solving combinatorial optimization problems using deep reinforcement learning and constraint programming, to extract the best differences and reduce the computation time for more difficult conditions. The goal is to improve the existing hybrid-cp-rl-solver tool to enable lightweight block cryptanalysis and propose an architecture for it.

## 研究の背景 ・ 目的

■背景

CRYPTO' 19のAron Gohr[1]の発表より、機械学習での軽量ブロック暗号解析が盛んに行われてきた。さらに、既存の方法では差分攻撃が有力であり、このSATやSMTを機械学習を用いて性能を高める試みは興味深いが研究例は少ない。

既存の解析ツールの問題点

- 高ラウンドだと精度の高い良い差分が出ない
- 解析時間が長い

```
Weight: 33 Time: 10905.08s
Weight: 34 Time: 12030.2s
Weight: 35 Time: 14823.18s
Weight: 36 Time: 17655.48s
Weight: 37 Time: 21182.52s
Weight: 38 Time: 31223.52s
```

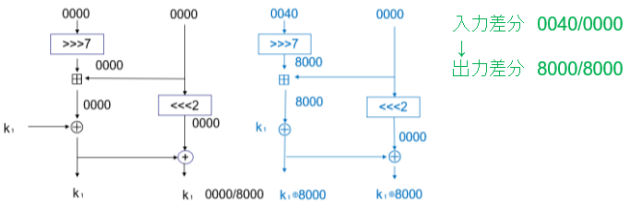
Cryptosmtで動かした、Speck,11round,wordsize32の値

■目標

深層強化学習と制約プログラミングを用いて組み合わせ最適化問題を解くツールを暗号解析向けに改良し、上記の問題を解決していく。

## 差分攻撃、SAT問題とは

■差分攻撃とは、ブロック暗号に対して有効な解読法。入力差分がどの様に出力差分に影響を及ぼすか考える。図に示すのは、Speckのラウンド関数である。




可能な差分 ← 制約 ← SATで記述

SAT問題を解くことが重要

■SAT問題とは、与えられた論理式が真と評価されるようなすべての変数の割り当てを見つけること。または、割り当てがない事を判断する事 $F := (x_1 \vee x_2) \wedge (\neg x_1 \vee \neg x_2)$

$x = True, x = False$

## 既存の攻撃アプローチ

■差分の特性を求めるsalsa20への攻撃の研究では、perlで論理式の前処理をし、CNF形式にしたものをSATソルバーに入力し、変数の割り当てから差分を得る。


■実際の差分の具体例（指標）

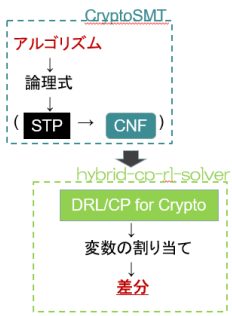
既存のSMT（SAT）を用いたツールにCryptosmtがある。上記の事前処理を含めpythonsのライブラリ化している。

https://github.com/kste/cryptosmt.git

## 検討している方法

Crypto-Hybrid-Cp-Rl-Solve

■Cryptosmt ソルバーはCryptominisat5がバックヤードで動いているため、それを組み合わせ最適化問題ツールであるhybrid-cp-rl-solverに置き換え暗号解析向けに改良する。




## 本研究の進め方

■CryptoSMTとhybrid-cp-rl-solverの互換性を高める

■高ラウンド、大サイズ、特に高ウェイトでも効率的に精度の高い差分を抽出出来るように改良する

- 制約プログラミングとしてdecodeが使われている為、Chuffedで再構築できないか？
- CP解決アルゴリズムの改良。
- DQN、PPO以外にも効率的なアルゴリズムはないか？

■対外的な目標（SUMMER SYMPOSIUMCSS 2022）

参考文献：Aron Gohr,Improving Attacks on Round-ReducedSpeck32/64 Using Deep Learning,CRYPT'19[1]Quentin Cappart, Combining Reinforcement Learning and Constraint Programming for Combinatorial Optimization,2020[2]