6ZA-07

深層学習を用いた現代暗号の解読手法

佐藤 駿介† 松澤 智史‡ 武田 正之‡

東京理科大学大学院 理工学研究科 情報科学専攻 †
東京理科大学 理工学部 情報科学科 ‡

1. 研究背景

近年，情報通信技術の発展によりIoTやクラウドといった技術が誕生し，生活の利便性が向上している．一方で，IoTやクラウドでは重要な情報をやり取りする必要があるので，サイバー攻撃のリスクは高まっている．サイバー攻撃への対策として，情報を安全に送受信する手段である暗号技術が存在する．

今利用されている暗号は，解読に必要な計算量が多項式時間に収まらないことを安全性の根拠としたものが多い．よくデータ通信に用いられる暗号であるRSAやAESは，解読に必要な計算量が莫大なことを安全性の根拠としている．しかし，近年の計算機の成長は著しく，解読に利用できる計算機の能力が増大することでそれらの暗号が危殆化する恐れがある．また，暗号の解読手法についても研究が進められており，暗号解読の一つのアプローチとして機械学習を用いた手法がいくつか提案されている．

本稿では，機械学習を用いることにより暗号解読が可能なことに加えて，現状の解読にかかる計算時間よりも早く解読できる可能性を，現代暗号を対象に実験をして検討する．

2. 関連研究と課題

2.1 機械学習を用いたDESの解読

ニューラルネットワークを用いた既知平文攻撃によりDESとTriple DESを解読する手法が提案されている[1]．この攻撃では暗号化にされた鍵を探索する必要はなく，平均2^{11}の平文と暗号文のペアから平均51分でDESの解読に成功している．同様の既知平文攻撃である線形解読攻撃[2]と比較すると，必要な平文と暗号文のペア数と必要な時間の両方が改善されているが，解読の成功率は約12%である．

2.2 深層学習を用いたエニグマの解読

時系列データを扱うのに長けたリカレントニューラルネットワーク(RNN)を用いて，ヴィジュネル暗号・エニグマといった換字式暗号を解読する手法が提案されている[3]．RNNの中でも長期的な依存関係を学習することのできるLSTM(Long Short Term Memory)ネットワークを用いて実装され，RNNが暗号のアルゴリズムを学習できること，解読に有用であることが示されている．

Alaniの論文[1]では線形解読法と比べて平文と暗号文のペアを少なくした解読を実現しているが，機械学習するにあたって明らかにデータが少ない．データの量を増やすことやネットワークの工夫によって，解読の成功率の向上が望める可能性がある．

また，Greydanusの論文[3]では一般に利用されていない暗号であるエニグマとヴィジュネル暗号に対してニューラルネットワークが有用なことが示されているが，RSAやAESのような現代で用いられている暗号に機械学習を用いた解読を試みた論文は少ない．

3. 提案手法

そこで本稿では，鍵とアルゴリズムが分割された現代暗号で，かつ共通鍵暗号であるDES，AES，RC4に対してニューラルネットワークを用いた解読が有用であるかを示すことを目的に解読モデルを実装した．DESとAESはブロック暗号なので平文の入力方法を指定する必要があるが，今回は一番単純なECBモードを用いる．ECBモードは平文に手を加えずに暗号化関数に入力するモードである．

言語はPythonで，ニューラルネットワークライブラリであるKerasを用いて実装した．実験1のRC4は自作の暗号化プログラムを，DESとAESは既存の暗号ライブラリであるpycrypto[1]を用いてデータセットを作成した．また，実験2以降は実験1で用いたライブラリではなく，自作であるDESの暗号化プログラムを用いた．

4. 実験及び結果

4.1 実験1

4.1.1 概要

共通鍵暗号であるRC4，DES，AESに対してニューラルネットワークによる既知平文攻撃による解読が有用であるかを示す．

同一の共通鍵における平文と暗号文のペアを大量に生成し，そのペアをデータセットとしてニューラルネットワークに学習させて解読モデルを実装した．入力は暗号文をビット列に変換したデータとし，出力は平文をビット列に変換したデータとする．ニューラルネットワークの入出力の形式を図1に示す．

4.1.2 結果

実験の結果，RC4の正解率が1.0，DESの正解率が0.5，AESの正解率が0.64となった．

Deciphering method of modern cryptography with deep learning

†Shunsuke Sato, ‡Tomofumi Matsuzawa, ‡Masayuki Takeda
{†Graduate School of Science and Technology, ‡Faculty of Science and Technology}, Dept.of Information Sciences, Tokyo University of Science

[1] https://github.com/dlitz/pycrypto

Copyright ©2019 Information Processing Society of Japan.
All Rights Reserved.

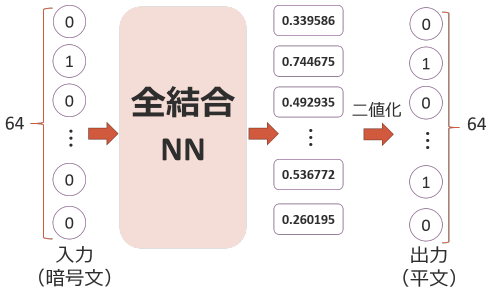

図 1: ニューラルネットワークの入出力のイメージ

4.2 実験 2

4.2.1 概要

実験 2 では DES 全体を模した NN ではなく，16 回のラウンドで用いられる暗号化関数をニューラルネットワークによって再現が可能か実装し検証した．

入出力は実験 1 と同様に入力を暗号文とし，出力を平文とする．サブキー 48 ビットを固定させて平文と暗号文のペアを生成した．

4.2.2 結果

実験の結果，平文の 1 ビット毎における正解率は 0.984 となった．

4.3 実験 3

4.3.1 概要

実験 3 では，平文と暗号文をセットとして入力として与え，サブキーを推測するニューラルネットワークを構築した．平文 32 ビットと暗号文 32 ビットを組み合わせた 64 ビットを入力として，推測したサブキー 48 ビットを出力とする．データセットはランダムにサブキーと平文を生成し，それらを DES によって暗号化した暗号文の三つをデータセットとした．

4.3.2 結果

実験の結果，サブキー 1 ビット毎に対する正解率は 0.817 となった．

5. 考察

5.1 実験 1

RC4 は暗号化のアルゴリズムから，排他的論理和をニューラルネットワークで構築するのと同義である．したがって，1.0 と高い成功率を出力した．DES はラウンドを 16 回繰り返すそのアルゴリズムの性質上ニューラルネットワークで再現するのが難しく，ランダムにビットを出力するのと変わらない結果となった．しかしながら，AES は 0.64 と DES を上回る成功率を出力した．これは本来であれば暗号の強度が高い AES が，機械学習において DES より解読されやすいといえる．

共通鍵暗号の解読をする上で，大まかなビット列を深層学習で解読し，残りのビット列を従来の線形解読で解読するといった手法が考えられる．この手法を用いることで本来解読にかかる時間を短縮することができる可能性がある．

5.2 実験 2

DES の一部分である暗号化関数を模したニューラルネットワークは実験 1 と比べて高い精度を示した．したがって，DES を既知平文攻撃で解くニューラルネットワークが実現できないのは，16 回のラウンドや縮約転置によってビットを攪拌する処理を模すことができないからといえる．しかし，実験 2 のように一部を再現することはできることから，DES の計算回路をそのままネットワークに取り込むことで精度の向上が見込める．現代暗号はアルゴリズムが公開されているので，アルゴリズムをネットワークに模すことができるならば，ネットワークが学習すべきは共通鍵の重みになる．

5.3 実験 3

DES のサブキーの推測は 0.817 の成功率であるが，暗号に関しては完全な復号が目標なので，高い精度であるとはいえない．このニューラルネットワークで 100 %に近い精度でサブキーを推測できるならば，元の共通鍵を復元できるので，より良い精度の向上を図る必要がある．

6. まとめ

本研究では，深層学習を用いることで暗号解読ができる可能性を示した．既知平文攻撃において DES より AES の精度が高いことから，機械学習による解読に対して撹拌を繰り返す DES は強いと考えられる．また，DES のラウンド関数やサブキーの推測などの別のアプローチから解読を実現できる可能性を示した．

参考文献

[1] Alani, Mohammed M. ”Neuro-cryptanalysis of des and triple-DES.” International Conference on Neural Information Processing. Springer, Berlin, Heidelberg, 2012

[2] Junod, Pascal. ”On the complexity of Matsui ’ s attack.” International Workshop on Selected Areas in Cryptography. Springer, Berlin, Heidelberg, 2001.

[3] Greydanus, Sam. ”Learning the Enigma with Recurrent Neural Networks.“ arXiv preprint arXiv:1708.07576 (2017).

Copyright ©2019 Information Processing Society of Japan.
All Rights Reserved.