様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　６ 年　 ６ 月 １１ 日現在

機関番号：１７１０４
研究種目：基盤研究(C)（一般）
研究期間：2021～2023
課題番号：２１Ｋ１１８９０

研究課題名（和文）暗号技術に対する機械学習や深層学習を用いた安全性評価のための攻撃手法の提案

研究課題名（英文）Proposal of attack methods using machine learning and deep neural network against cryptographic techniques for security evaluation

研究代表者

荒木　俊輔（Araki, Shunsuke）

九州工業大学・大学院情報工学研究院・准教授

研究者番号：２０３３２８５１

交付決定額（研究期間全体）：（直接経費）　　3,200,000円

研究成果の概要（和文）：近年注目を集める機械学習や深層学習はランダムな事象に対する推論が困難であるという特徴に着目して、共通鍵暗号や擬似乱数生成器などの暗号技術への安全性評価に用いることを考えた。その第一段階として、これらの技術を用いた攻撃手法に関する研究を行った。共通鍵暗号に対する攻撃では、暗号強度が弱くなるように暗号仕様を変更した制限付き状態ではあるが、機械学習や深層学習を用いて、平文と暗号文のみの入力に対する鍵識別攻撃や、暗号文のみの入力に対する平文解読攻撃が可能であることを確認した。また、擬似乱数生成でよく利用されていた線形合同法に対して、深層学習にて、次時刻の出力値を予測できることが分かった。

研究成果の学術的意義や社会的意義
本研究では、出力がランダムである事が期待される暗号技術に対して、ランダムな事象が苦手な機械学習や深層学習を攻撃手法として用いることで、これまで見つけることができなかった何かしらの「偏り」を見つけ出すことができた。
その結果、これら機械学習や深層学習が、暗号技術の安全性評価にも活用できることを明らかにした。

研究成果の概要（英文）：Focusing on features that machine learning and deep learning, which have attracted much attention for many research fields in recent years, are difficult to inference about random events, we thought these technologies are used for security evaluations for cryptography. As the firs step of our research, we studied attack methods using these techniques against cryptographic techniques such as common-key cryptography and pseudo-random number generators. In the attack on common-key cryptography, we confirmed that a key identification attack against input of only plaintext and ciphertext and a plaintext decryption attack against input of only ciphertext are possible using machine learning and deep learning, although with the restriction that the cryptographic specifications are modified to weaken the cryptographic strength. We also found that deep learning can predict the output at the next time for the linear congruence method, which was often used in a pseudorandom number generation.

研究分野：情報セキュリティ

キーワード：機械学習　深層学習　AES　共通鍵暗号　軽量暗号　擬似乱数生成　線形合同法

様　式　Ｃ－１９、Ｆ－１９－１（共通）

１．研究開始当初の背景

一般的に「**機械学習や深層学習はランダムに振る舞う問題が苦手である**」と言われていることに注目したことが、本研究の着想の原点である。この点に着目すると

・機械学習や深層学習は、ある事象に「偏り」があるかを判別可能

と言い換えることができることに気づいたのが、本研究の着想に至った経緯である。

これまで、我々は、計算機実装によるカオス写像を用いた擬似乱数生成器に関する研究を行ってきた。そこでは、0 と 1 の出現頻度など**統計的な振る舞い**が、良質な擬似乱数生成に密接にかかわっている。これまで利用してきた、米国標準技術研究所(NIST)による乱数検定ツールでは、擬似乱数として満たすべき統計量を定義し、理論的な分布に沿っているかを検定している。言い換えると、定義できない乱数性については、評価していないことを意味する。一方、機械学習ではハミング重みなどの何らかの指標を与える必要はあるが、厳格に定義せずにパターン学習が可能であり、「偏り」を見つけ出す可能性が存在する。

近年、機械学習や深層学習は静止画像や動画像のオブジェクト検出や、囲碁や将棋など、様々な分野で活用が進んでいる。その一方で、株価などの予想は、ランダムな振る舞いであり単純な適用は困難だといわれている。つまり、**本研究課題は挑戦的な取り組み**であることを示している。

２．研究の目的

研究目的は、「**暗号技術に対する機械学習や深層学習を用いた安全性評価のための攻撃手法の提案**」である。暗号技術の中でも、特に共通鍵暗号や擬似乱数生成器に対して、以下のことを実施する。

課題 1: 何らかの「偏り」を持つ統計量の調査
課題 2: 鍵や初期パラメータなどの情報の分類器の作成

本研究は、「**一般的に、機械学習や深層学習はランダムに振る舞う問題が苦手である**」こと、「**共通鍵暗号や擬似乱数生成器は、0 や 1 のビット出現頻度等の偏りがないことを目指して設計されている**」こと、これら 2 つのことに着目したものである。まず、**課題 1** として、一般的にはランダムな事象に向いていないとされる機械学習や深層学習を用いて、共通鍵暗号や擬似乱数生成器の何かしらの「偏り」をもつ統計量を調査する。特に、**課題 2** は、偏りを持つ統計量を用いて、共通鍵暗号であれば鍵を、擬似乱数生成器であれば初期パラメータを、その統計量の偏りに応じたグループに分類できる分類器を提案する。

３．研究の方法

本研究は、最終的なゴールである

・共通鍵暗号・擬似乱数生成器に対する、機械学習・深層学習を用いた評価手法の確立

の達成に向け、共通鍵暗号や擬似乱数生成器に対する、以下の研究課題の実施が不可欠だと考えている。

課題 1: 何らかの「偏り」をもつ統計量の調査
課題 2: 共通鍵暗号・擬似乱数生成器における共通鍵・初期値等の分類器の作成
課題 3: 共通鍵暗号・擬似乱数生成器における共通鍵・初期値等に対する攻撃手法の提案
課題 4: 共通鍵暗号・擬似乱数生成器における安全性の評価手法の提案

第一段階として、本研究期間においては、**課題 1 と課題 2 を実施**する。特に、共通鍵暗号として、AES に着目して研究を進める。これに加え、IoT などの低リソースデバイスでの実装が想定されている軽量暗号に対しても同様の研究を行う。特に、CRYPTREC 暗号技術ガイドライン(軽量暗号)[引用文献:①]で議論されている軽量暗号に着目する。一方、擬似乱数生成器としては、AES のカウンタモード、我々がこれまで研究を行ってきた、計算機上のカオス写像による擬似乱数生成器や、平方剰余を用いた幾何的系列を対象とする。

課題 1: 共通鍵暗号・擬似乱数生成器における何らかの「偏り」をもつ統計量の調査

課題 1 は、最終的なゴールである課題 4 を実現するための、本研究におけるメインテーマである。本研究の着眼点は、「**機械学習や深層学習はランダムに振る舞う問題が苦手である**」こと、「**共通鍵暗号や擬似乱数生成器は「偏り」の無い情報の出力を目指した処理である**」こと、「**そのような機械学習や深層学習により高い正答率を得られれば、そこに何かしらの『偏り』が存在する**」ことである。機械学習や深層学習を用いた手法を検討する上で、様々な「偏り」を表す統計量や表現形式があるため、研究期間全体を通じて実施する。

```
Cipher(data){
    AddRoundKey(data,0);
    for(i=1; i<nr; i++){
        SubBytes(data);
        ShiftRows(data);
        MixColumns(data);
        AddRoundKey(data, i);
    }
    SubBytes(data);
    ShiftRows(data);
    AddRoundKey(data, i);
}
```

図 1 AES のメイン処理

AES を例にとり説明する。
図 1 に示すように、AES の暗号化処理は 4 つの関数(SubBytes 関数、MixColumns 関数、ShiftRows 関数、AddRoundKey 関数)により構成され、これらの関数の出力は次に呼び出される関数の入力となっている。図 1 の繰り返し処理が 1 ラウンドを構成し、複数ラウンド実行される。そのため、平文と各地点の関数の出力は、無関係に見えることが望ましい。その関係性を評価するために、機械学習により以下の実験を行う。

- **「鍵 ID、平文、ある地点の関数の出力、それら 2 つの間の関係性」を訓練データとした学習**
- **「平文、ある地点の関数の出力、それら 2 つの関係性」による鍵 ID の正答率の調査**

最初に、どの要素が解答に影響を与えたのかを視覚化可能な、ランダム・フォレストを利用する。次に、そこで特定した要素が具体的にどのような影響を与えているのかを分析する。複数の要素が解答に影響を与えることが分かった場合、それらの組み合わせで、さらに細かな鍵の特定が可能かを調査する。

課題 2: 共通鍵暗号・擬似乱数生成器における共通鍵・初期パラメータの分類器の作成

課題 1 により得られた知見を用いて、分類器を構成する。課題 2 は、課題 1 の結果を受け行う。そのため、研究分担者と連携を密に取り、課題 1 による成果を受け取りつつ、本課題を進める。
　例えば、この分類器により 2 つのグループに鍵・初期パラメータが分けられると、それらの 1 ビット分の情報が分かったことに等しい。そこで、

- **「偏り」の分析**
- **同じ「偏り」を持つ鍵・初期パラメータの分析**
- **分析結果を用いた、「偏り」もしくは鍵・初期パラメータの分類器の構成**

を実施する。これらの分析結果の中で、互いに独立なものを組み合わせ、より細かく分類することで、結果的に探索する鍵・初期パラメータの探索範囲を狭めることが可能となる。

４．研究成果

(1) 標準共通鍵暗号 AES(Advanced Encryption Standard)に対する攻撃
　AES に対する攻撃手法として、機械学習を用いた直接的な暗号文を解読する攻撃は現実的ではないため、基礎的な実験として、鍵識別実験(二つの異なる鍵に対して、平文と暗号文対を計算)に取り組んだ。しかしながら、ランダム・フォレスト等の基本的な手法を用いて仕様通りの AES に対して鍵識別実験を行ったが、鍵識別ができなかった。また、攻撃の可能性を高める為に AES の暗号強度を弱める、繰り返し処理(ラウンド)回数を減らして実験を行ったが、鍵識別は成功しなかった。つまり、実験環境下では機械学習・深層学習が何かしらの「偏り」を見つけることができないことが分かった。
　その一方で、AES の安全性評価に繋がる、異なるアプローチを取った。AES は 4 つの関数を交互に作用させることにより暗号化されるが、その内の一つの関数を無効化する特別な AES 暗号化処理における鍵識別実験を行った。SubBytes 関数および MixColumn 関数を実行しない場合に、高い確率で鍵識別が成功する良い結果を得た。つまり、機械学習・深層学習を用いた攻撃手法に対して、SubBytes 関数と MixColumn 関数の両者のデータの攪拌手法が暗号強度を高めていることが分かった。

(2) 旧標準共通鍵暗号 DES(Data Encryption Standard)に対する攻撃
　AES にて採用されていた SPN 構造とは異なる、Feistel 構造を持つ旧標準暗号である共通鍵暗号 DES に対する機械学習を用いた攻撃手法として、以下の実験を行った。
・鍵識別実験:
　AES で実施した内容と同様の内容で、DES に対して本実験を実施した。ランダムに選択した 2 つの鍵に対する実験、および暗号文に望ましくない振る舞いを示す弱鍵とランダムな鍵のペアに対する実験を行ったが、鍵識別を有意な確度で正解することはできなかった。

・平文推測実験:
ランダムに選ばれた鍵に対してランダムに選んだ平文から暗号文を作成して、その平文・暗号文ペアを学習させ、暗号文に対する平文推測実験を行った。フル規格の 16 ラウンドの DES に対しては有効な結果を得ることができなかった。一方、1 および 2 ラウンドの DES に対して、平文推測が可能な自明なビット位置以外の少数のビットも高い確率で推測できることが分かった。
・アンサンブル手法を用いた平文推測実験:
2 ラウンドの DES に対して、学習データの学習順序を変更すると、正答率が異なる事が分かった。そこで、同一の学習データに対して、順序を変えた複数の学習を行い、それらから正答率が高いビット位置の結果を利用するアンサンブル手法を用い、2 ラウンドの DES に対して、平文推測攻撃が可能であることが分かった。
これらの実験により、既に利用が推奨されない暗号手法であっても、機械学習・深層学習を用いた単純な攻撃は通用しないことが分かった一方で、ラウンド数を小さくした場合は、復号が可能な自明なビット以外でも、高い確率で復号できることも分かった。

(3) 軽量暗号に対する平文解読実験
軽量暗号の一つである Midori に対して、平文推測実験を行った。また、Midori は AES と同様に SPN 構造を持っているため、構成要素である 4 つの関数を一つずつ無効化する AES に対して実施した同様の平文推測実験を行った。平文推測実験では、仕様書通りのフルラウンドでの平文、暗号文対に対するニューラルネットワークに対する学習及びそのモデルに対する暗号文を入力した際の平文の正答率は 5 割であり、失敗した。その一方で、ラウンド数を減らしていき同実験を行ったところ 1 ラウンドの Midori では多くのビットにおいて正答率が 5 割を超える良い結果を得た。また、関数を一つずつ無効化した Midori に対する平文推測実験では特に MixColumn 関数を無効化した場合、ほぼ正答できる結果を得た。その結果、ニューラルネットワークを用いた平文推測攻撃に対して MixColumn 関数が重要である事が分かった。
Midori は MixColumn 関数が重要である結果を得たように、SPN 構造の場合は、関数の構成法が重要である事が分かった。

(4) 擬似乱数生成器に対する次ビット予測実験
学習データとして、擬似乱数ビット列を用いて、過去の出力と正解ラベルとしての次刻の 1 ビットとし、テストデータとして過去の出力を与え次刻の 1 ビットを予測する実験を行った。gcc の rand 関数や microsoft C/C++の rand 関数で利用されていたパラメータに対して、十分な学習データ量があれば、高い確率で次刻の 1 ビットを予測することに成功した。
さらに、どのビットの予測精度が高いのか調査したところ、gcc の rand 関数などのパラメータに対して、次刻の出力のビット毎の予測成功確率を求めたところ、下位 10 ビット程度が高い予測精度を得ていることが分かった。これらの線形合同法では 2 の「ビット位置」乗の周期がある事が知られており、周期が短いビット位置の成功確率が高いことが確認できた。
この実験により、出力値としての周期が長くても、出力値のビット位置に着目した周期性を機械学習・深層学習は、学習が可能である事を示しているため、擬似乱数生成器の構成法について、出力値のビット位置に依存した周期を持たないような、新たな設計指針を得た。

(5) 機械学習・深層学習を用いた次ビット予測を困難にする擬似乱数生成器に関する研究
線形合同法は、出力ビット位置に依存した周期性のために高い確率で次ビットを予測できることが分かった。その為に、この種の攻撃に強いことを期待して、いくつかの擬似乱数生成器に関する研究を行った。
整数上のロジスティック写像には出力ビット位置に特有の 0/1 の偏った出現確率を持つ問題点に対して、ロジスティック写像を複数組み合わせえることによって、ビット毎の 0/1 出現確率のバランスを良くするための構成法を提案した。また、定義域内に複数のロジスティック写像を重ならないように配置するピースワイズ・ロジスティック写像に関して、整数化した上で、乱数性を評価して、良い結果を得た。
二拠点間で乱数系列を共有するための手法としてカオス写像として知られているローレンツ方程式を用いた鍵共有法が提案されているが、その実装が浮動小数点演算で定義されている問題に対して、整数化を行い、それまでと同様の鍵共有などが可能である事を示した。
シンプルな二次関数を用いた手法とは異なる、迷路作成手法を用いることで、ファミリー数を多く取れる利点を持つ擬似乱数生成器を提案した。

<引用文献>
① CRYPTREC 軽量暗号ワーキンググループ, “CRYPTREC 軽量暗号ガイドライン(軽量暗号),” https://www.cryptrec.go.jp/report/cryptrec-gl-2003-2016jp.pdf, 2016.

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計15件（うち招待講演　0件／うち国際学会　8件）

１．発表者名 野口 亮祐，荒木 俊輔，宮崎 武，上原 聡，碓崎 賢一
２．発表標題 線形合同法における周期性とニューラルネットワークによる予測精度に関する考察
３．学会等名 2023年暗号と情報セキュリティシンポジウム(SCIS2023)
４．発表年 2023年

１．発表者名 R. Inoue, T. Miyazaki, S. Uehara, S. Araki and Y. Nogami
２．発表標題 A study on parameters of piecewise logistic map over large integers and processing time
３．学会等名 Proc. of 2022 International Conference on Consumer Electronics - Beitou (ICCE-TW)（国際学会）
４．発表年 2022年

１．発表者名 井上 凌，宮崎 武，荒木 俊輔，上原 聡
２．発表標題 整数上のPLMを用いた擬似乱数系列の4 つのパラメータに対する乱数性の一考察
３．学会等名 第8回有限体理論とその擬似乱数系列生成への応用ワークショップ予稿集
４．発表年 2022年

１．発表者名 藤井 博希，上原 聡，宮崎 武，荒木 俊輔，日下 卓也，野上 保之
２．発表標題 2つの整数上のロジスティック写像を用いたバランスの良い擬似乱数生成法に関する一考察
３．学会等名 第45回情報理論とその応用シンポジウム予稿集
４．発表年 2022年

１．発表者名
A. Inomata, S. ARAKI, K. Kakizaki

２．発表標題
A Study on Use of Machine Learning to Evaluate the Security of Common Key Cryptosystem

３．学会等名
2021 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW)（国際学会）

４．発表年
2021年

１．発表者名
野口亮祐，荒木俊輔，宮崎武，上原聡，碇崎賢一

２．発表標題
線形合同法による擬似乱数に対するニューラルネットワークを用いた予測

３．学会等名
第7回有限体とその擬似乱数生成への応用ワークショップ

４．発表年
2021年

１．発表者名
M. Kawano, S. Peng, S. Araki, K. Kakizaki

２．発表標題
A Study on Guessing plaintexts by Neural Network against Data Encryption Standard (DES)

３．学会等名
2023 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW)（国際学会）

４．発表年
2023年

１．発表者名
J. M. Mwaura, S. Araki, K. Kakizaki

２．発表標題
A Study on DDoS Attacks Detection on IoT Devices Using Machine Learning for Microcontrollers

３．学会等名
IEEE 42nd International Conference on Consumer Electronics（国際学会）

４．発表年
2024年

１．発表者名
H. Fujii, S. Uehara, T. Miyazaki, S. Araki, Y. Nogami

２．発表標題
Some properties of well-balanced sequences obtained from two logistic maps over integers

３．学会等名
2023 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW)（国際学会）

４．発表年
2023年

１．発表者名
藤井 博希，宮崎 武，荒木 俊輔，上原 聡，野上 保之

２．発表標題
2つの整数上のロジスティック写像を用いた擬似乱数生成法の統計的乱数性に関する一考察

３．学会等名
第9回有限体理論とその擬似乱数系列生成への応用ワークショップ

４．発表年
2023年

１．発表者名
高市 康平，顔 綿柱，荒木 俊輔，宮崎 武，上原 聡

２．発表標題
研究紹介:動的同期カオスベースランダム鍵を用いたビデオ/オーディオストリーミング用暗号システム

３．学会等名
第9回有限体理論とその擬似乱数系列生成への応用ワークショップ

４．発表年
2023年

１．発表者名
藤井 博希，森脇 圭祐，宮崎 武，荒木 俊輔，上原 聡，野上 保之

２．発表標題
2つの整数上のカオス写像を用いた擬似乱数系列の乱数性に関する一考察

３．学会等名
第46回情報理論とその応用シンポジウム

４．発表年
2023年

１．発表者名
Y. Takeuchi, I. Maebayashi, M. A. Ali, T. Kusaka, Y. Nogami, Y. Kodera

２．発表標題
A Consideration of Parameters for a Nonlinear Filter Generator and its Linear Complexity Profile

３．学会等名
2023 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW)（国際学会）

４．発表年
2023年

１．発表者名
A. Miyoshi, K. Ikesaka, M. A. Ali, Y. Kodera, T. Kusaka, Y. Nogami

２．発表標題
A Consideration of Averaging the Calculation Cost of CVMA for A Secure Session based Data Transmission

３．学会等名
2023 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW)（国際学会）

４．発表年
2023年

１．発表者名
R. Kato, T. Manabe, S. Kanzawa, S. Huda, Y. Kodera, T. Kusaka, Y. Nogami

２．発表標題
Reducing Fruitless Cycles in Pollard's Rho Method with SFM for Efficient ECDLP Attacks on BN Curves

３．学会等名
The 39th International Technical Conference on Circuits/Systems, Computers, and Communications（国際学会）

４．発表年
2024年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	野上　保之 (Nogami Yasuyuki) (60314655)	岡山大学・自然科学学域・教授 (15301)	

６．研究組織（つづき）

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	上原　聡 (Uehara Satoshi) (90213389)	北九州市立大学・国際環境工学部・教授 (27101)	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関			
その他の国・地域	国立勤益科技大学			