Vol.2021-DPS-186 No.67
Vol.2021-CSEC-92 No.67
2021/3/16

ニューラルネットワークを用いた 軽量ブロック暗号 PRESENT の解析

勝田耕作[1]　五十嵐保隆[1]　金子敏信[1]

概要：PRESENT は 2007 年に Bogdanov によって提案された軽量ブロック暗号である．ニューラルネットワークは大量のデータを学習させることにより，とある入力値に対し理想的な値を出力する学習器を作り出す技術である．暗号解析においては，攻撃対象の暗号の内部構造が未知であっても，入出力データを学習データとして用いることで関係を予測することが可能である．本稿ではニューラルネットワークを用いた解析を PRESENT に適用した．具体的に行った実験は平文予測攻撃，鍵スケジュール解析である．平文予測攻撃は 1200000 組の(暗号文，平文)のデータセットを学習に用いることで，暗号文から平文のランダムでない予測が 4 段まで実現できることを示す．鍵スケジュール解析は多くて 1000 組の(最終段段鍵，秘密鍵)のデータセット，もしくは(最終段鍵スケジュール内部状態，秘密鍵)のデータセットを学習データに用いることで，最終段の鍵データから秘密鍵のランダムでない予測がフルラウンド 31 段の PRESENT 鍵スケジュールにおいて実現できることを示す．

キーワード：ニューラルネットワーク．軽量ブロック暗号，PRESENT

Neural Network based cryptanalysis of Lightweight block cipher PRESENT

Kosaku Katsuda[†1]　Yasutaka Igarashi[†1]
Toshinobu Kaneko[†1]

Abstract: PRESENT is a lightweight block cipher proposed by Bogdanov in 2007. A neural network can create a function that outputs an ideal value for a certain input value by training a large amount of input / output data. In cryptanalysis, even if the internal structure of the attack target cipher is unknown, it is possible to predict the relationship between known input and unknown output by using the input / output data as learning data. In this paper, we applied the analysis using a neural network to PRESENT. We implement plaintext prediction attacks and key schedule analysis. The plaintext prediction attack shows that non-random prediction of plaintext derived from ciphertext can be realized for up to 4-round PRESENT by using 1,200,000 sets of (ciphertext, plaintext) datasets for training. Key schedule analysis can be performed with the final state key data by using at most 1,000 sets of (final round key, master key) data or (final key register, master key) data as training data. We show that non-random prediction of the master key can be realized in the 31-round PRESENT key schedule function.

Keywords: Neural Network, Lightweight block cipher, PRESENT

1. 序論

PRESENT は 2007 年に Bogdanov によって提案された軽量ブロック暗号である．ニューラルネットワークは大量のデータを学習させることにより，とある入力値に対し理想的な値を出力する学習器を作り出す技術である．暗号解析においては，攻撃対象の暗号の内部構造が未知であっても，入出力データを学習データとして用いることで入出力関係を予測することが可能である．

本稿ではニューラルネットワークを用いた解析を PRESENT に適用した．具体的に行った実験は平文予測攻撃，鍵スケジュール解析である．平文予測攻撃は 1200000 組の(暗号文，平文)のデータセットを学習に用いることで，暗号文から平文のランダムでない予測が 4 段まで実現できることを示す．鍵スケジュール解析は多くて 1000 組の(最終段段鍵，秘密鍵)のデータセット，もしくは(最終段鍵スケジュール内部状態，秘密鍵)のデータセットを学習データに用いることで，最終段の鍵データから秘密鍵のランダムでない予測がフルラウンド 31 段の PRESENT 鍵スケジュールにおいて実現できることを示す．

1 東京理科大学理工学研究科電気工学専攻
Tokyo University of Science, Graduate School of Science and Technology, Department of Electrical Engineering

2. 暗号の評価方式

安全な暗号が満たす性質の一部として，以下のような性質がある．

- 情報理論的安全性
- 計算量的安全性
- 識別不可能性

本研究では識別不可能性に基づく安全性評価を行うため，以下にて説明する．

2.1 識別不可能性

識別不可能性とは，ある暗号器をランダムオラクルと区別できないという性質である．ただし，暗号器は内部構造

Vol.2021-DPS-186 No.67
Vol.2021-CSEC-92 No.67
2021/3/16

が分からないブラックボックス状態であるとする．ランダムオラクルとは理想的な乱数のことを意味し，いかなるデータの偏り，法則性が現れないものとする．

つまり，ある暗号器においてデータの偏り，法則性等が現れてしまうと，識別不可能性に反することになる．したがって，安全な暗号もしくは安全な暗号の使い方とは言えなくなる．

3. ニューラルネットワーク

ニューラルネットワークは人工知能，機械学習技術の一つである．大量のデータを学習させることで，データの特徴や法則性を導き出し，とある入力値に対して理想的な出力をする学習器へと変化する．

3.1 教師あり学習

本研究では，ニューラルネットワーク，機械学習技術の中でも教師あり学習を用いた．教師あり学習とは，ある関数において入力のデータと予め用意した正解値の出力データ(教師データ)を用いて関数を近似した学習器を生成する手法である．学習器を生成するにあたって，トレーニングとテストという 2 つのステップを経由する．

3.2 パーセプトロン

パーセプトロンとはニューロンを関数化した数理モデルである．

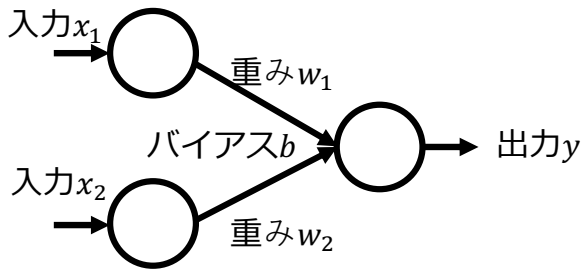

図 1　パーセプトロン

図 1 の場合では，2 変数入力 x_1, x_2 となっており，情報の伝わりやすさを表す重み w_1, w_2，またしきい値となるバイアス b というパラメータで構成されている．その出力 y は式(1)の通りで表すことができる．

$$y=a(w_1x_1+w_2x_2+b) \quad ...(1)$$

ここで関数 a(x)は活性化関数を表しており，x=0 をしきい値として値を出力しだすような関数である．図 2 に，活性化関数の一部である Step 関数，Sigmoid 関数，ReLU 関数を示す．

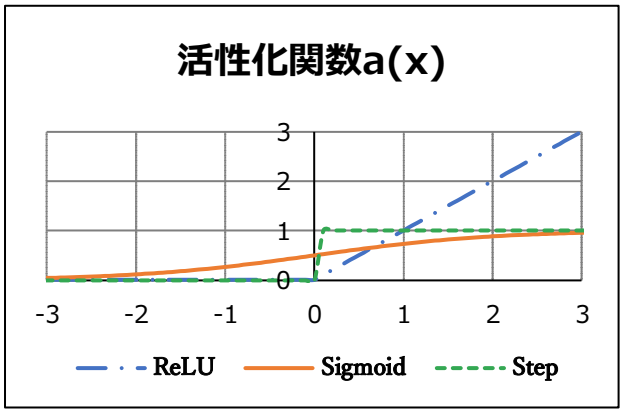

図 2　活性化関数の例

3.3 ニューラルネットワークの構造

ニューラルネットワークの構造は，図 3 のようにパーセプトロンを多層に重ねたものとなっている．

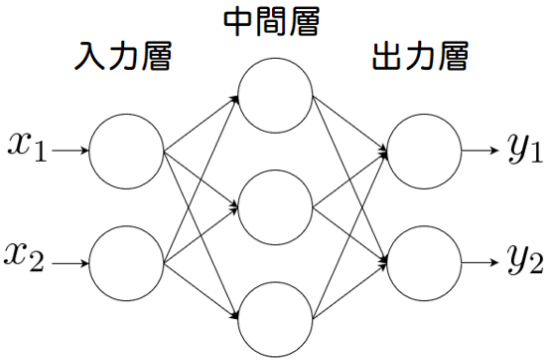

図 3　ニューラルネットワークの構造

また，各パーセプトロン間には 3.2 節のようなパラメータが存在しており，そのパラメータを決定する作業が学習に当たる．

3.4 学習

学習の手順は教師あり学習に基づき，トレーニングとテストの 2 つのフェーズに分けて行う．それに伴いデータもトレーニング用とテスト用に分けて使用する．

3.4.1 トレーニングの手順

トレーニングは図 4 に基づき以下の手順で行う．

①ニューラルネットワークのパラメータをランダムに初期化する．

②トレーニング用入力データを与えて予測値を計算する．なおデータは一括で使わずに一定数(バッチサイズ)に分割して使用する．

③予測値とトレーニング用教師データとの誤差を導出する．その際に用いるのが損失関数である．

④パラメータの更新を，手順 3 で得られる誤差が小さくなるように行う．その際に用いるのが最適化関数である．

⑤手順 2 に戻り，残りの分割データに対しても 2~4 の処理を行う．

Vol.2021-DPS-186 No.67
Vol.2021-CSEC-92 No.67
2021/3/16

⑥手順 2~5 を繰り返す．繰り返しの回数をエポック数という．

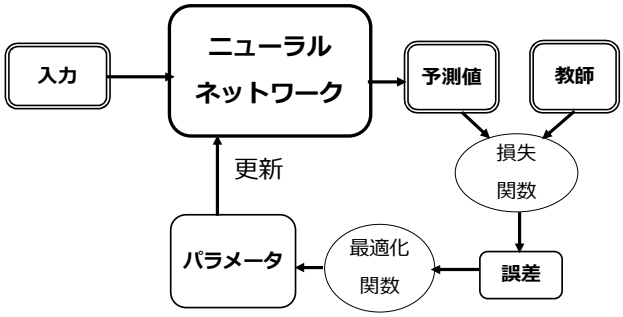

図 4　ニューラルネットワークのトレーニング手順

なお，本稿では損失関数として MSE(最小二乗誤差)を用いる．
また，本稿では最適化関数として Adam を用いている．Adam は他の最適化関数と比べて収束が早いとされている．また，最適化関数においてニューラルネットワークのパラメータを一度にどの程度変更するかを表す値を学習率 η で表す．η は $0<\eta<1$ の範囲を取る．

3.4.2　テストの手順

トレーニングフェーズで構築したニューラルネットワークモデルにテスト用入力データを与えて予測値を計算する．そして得られた予測値がテスト用教師データと十分に一致しているかどうか確かめる．場合によってはトレーニングフェーズに戻る，もしくはニューラルネットワークの層の数やニューロン数等を変更してからトレーニングフェーズに戻る．

4.　軽量ブロック暗号 PRESENT

PRESENT は 2007 年に Bogdanov らによって開発された軽量ブロック暗号である．国際標準化機構(International Organization for Standardization)および国際電気標準会議(International Electrotechnical Commission)において軽量暗号の国際標準に含まれており，最新の軽量暗号のセキュリティを測定するための基準となっているブロック暗号である．

4.1　PRESENT の全体構造

PRESENT の全体構造は図 5 のようになる．ブロック長は 64 ビット，秘密鍵長は 80 ビットとなっている．全体の手順としては，まず秘密鍵が鍵スケジュール部に入力され，段関数と呼ばれる繰り返し関数を繰り返しながら 64 ビットの段鍵 $K_1, K_2, \ldots, K_{32}$ を抽出していく．次に平文をデータランダム化部に入力し，段関数処理を繰り返して暗号文を出力する．

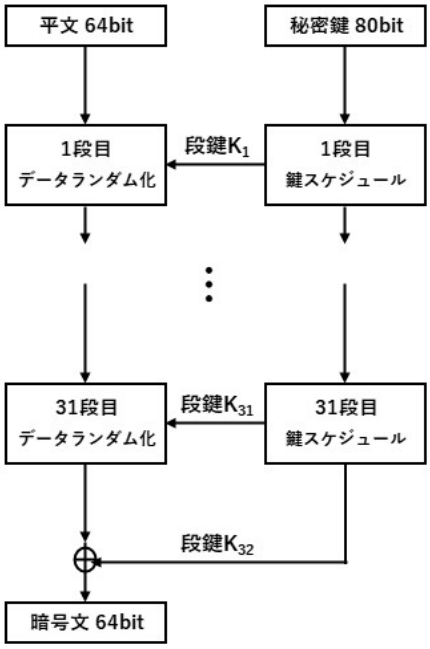

図 5　PRESENT の全体構造

4.2　PRESENT のデータランダム化

図 6 に PRESENT のデータランダム化部の段関数を示す．まず，入力のデータに段鍵 K_r (r=1, 2, …, 32)が XOR される．次に表 1 に表す S-Box と呼ばれる関数を用いて 4 ビットごとの非線形変換を行う．最後に 1 ビットごとの転置処理を行い段関数処理を終える．

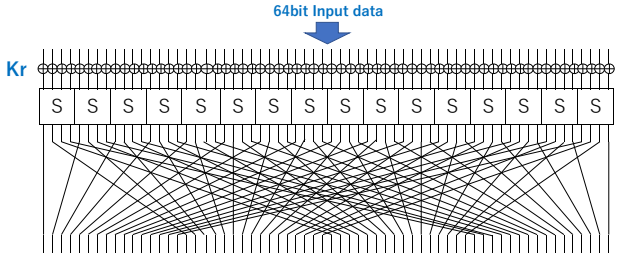

図 6　PRESENT のデータランダム化部の段関数

表 1　PRESENT の S-Box(16 進数)

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S[x]$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

4.3　PRESENT の鍵スケジュールの段関数

図 7 に PRESENT の鍵スケジュール部の段関数を示す．まず，79~16 ビット目の合計 64 ビットを段鍵として抽出する．次に，左に 61 ビット巡回シフトをする．次に 79～76 ビット目に表 1 の S-Box 変換を適用する．最後に 19～15 ビット目に現在の段を 2 進数に直して XOR を行う Round Counter 処理を行い，段関数処理を終える．

Vol.2021-DPS-186 No.67
Vol.2021-CSEC-92 No.67
2021/3/16

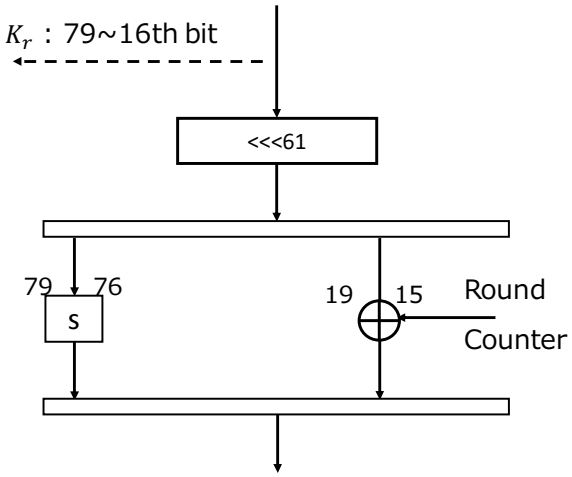

図 7　PRESENT の鍵スケジュールの段関数

5. 実験とその結果

本研究ではニューラルネットワークを用いて以下の実験を行った．

1. PRESENT に対する平文予測攻撃
2. PRESENT の鍵スケジュール解析

そして，一貫してトレーニングを終えた学習器の正確さを正答率 acc で表す．ただし，acc は 1 ビットの正答率を表すものとする．acc は式(2)で定義される．

$$acc=a/n \quad \ldots(2)$$

ただし，a を予測値と教師データ値の一致数，n をテストデータ数とする．

なお，正答率 acc が 0.5 を上回った状況を”ランダムではない精度の予測”と定義する．これが実現すると，2.1 節の識別不可能性が崩れ，安全な暗号もしくは安全な暗号の使い方と呼ぶことができなくなる．

5.1 【実験 1】PRESENT に対する平文予測攻撃

5.1.1 攻撃の概要

図 8 に示すようにこの攻撃は平文と暗号文の組がある程度入手できる状況を考える(それを既知平文攻撃または既知暗号文攻撃と呼ぶ). 用いる学習データセットは入力データが暗号文，教師データが平文であり，作成する学習器は暗号文から平文を予測する関数である．これによりもたらされる脅威は，学習データ外の暗号文(公開情報)から未知である平文をランダムでない精度で予測されてしまうことである．

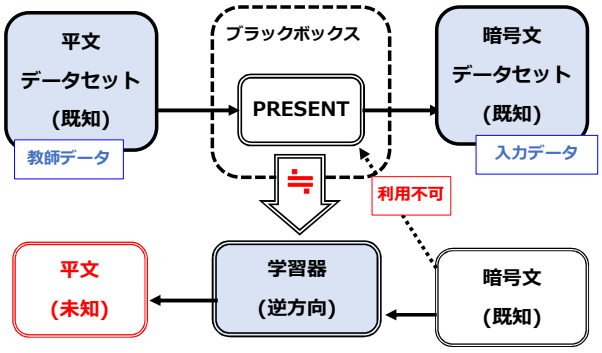

図 8　PRESENT に対する平文予測攻撃

5.1.2 実験 1 の手順

以下の手順①～⑤を 1～5 段に削減した PRESENT に対して行った．

① 秘密鍵をランダムに定める．
② 平文を 1200000 個ランダムに定める．
③ ②の平文を暗号化，(暗号文，平文)のデータセットを 1200000 組生成する．
なお，秘密鍵は全て①で定めたものを用いる．また，データセットのうち 1000000 組をトレーニングデータ，200000 組をテストデータとする．
④ トレーニングデータを用いてトレーニングを行う．
⑤ テストデータを用いて各ビットの正答率 acc の平均を求める．

この①～⑤の手順を全部で 3 回行い，全試行の acc の平均を最終的な値とする．この実験を行うことで，PRESENT において暗号文から平文のランダムではない精度の予測が何段まで実現するかを明らかにすることができる．

5.1.3 実験 1 の学習モデル

実験 1 のニューラルネットワークの構造，ハイパーパラメータは表 2 の通りである．

表 2　実験 1 の学習モデル

構造	入力層，中間層×3，出力層
パーセプトロン数	64 -128-256-128 -64
活性化関数	LeakyReLU
損失関数	MSE(最小二乗誤差)
最適化関数	Adam
学習率	0.001
バッチサイズ	200
エポック数	300

Vol.2021-DPS-186 No.67
Vol.2021-CSEC-92 No.67
2021/3/16

5.1.4 実験 1 の結果

各ビットの正答率 acc の平均は表 3, 図 9 の通りである.

表 3 【実験 1】平文予測攻撃の結果(各ビット acc の平均)

段数	正答率 acc
1	1.000
2	0.961
3	0.596
4	0.526
5	0.500

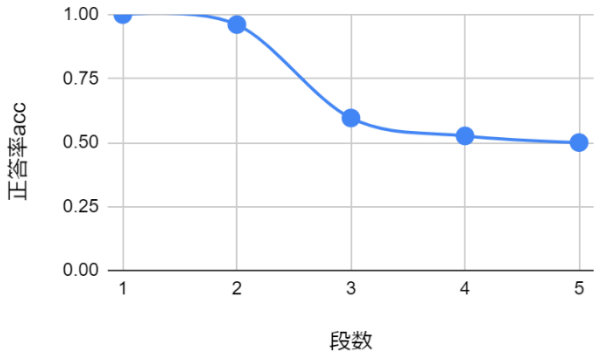

図 9 【実験 1】平文予測攻撃の結果(各ビット acc の平均)

これより，段数が増えるほど正答率 acc は下がることがわかる．また 1〜4 段までは正答率が 0.5 より高い確率，5 段では正答率が約 0.5 となることが分かる．この結果より，PRESENT において 1200000 組のデータセットを用いる場合では 4 段まで暗号文から平文のランダムでない精度での予測が可能であることが分かった.

5.2 【実験 2】PRESENT の鍵スケジュール解析

5.2.1 手法の概要

この手法は, 図 10 に示すように秘密情報のうち秘密鍵と最終段段鍵もしくは最終段鍵スケジュール内部状態値をある程度入手できる状況を仮定する．暗号攻撃において秘密鍵や内部情報が既知となる攻撃条件は存在しないため，この解析は攻撃ではなく鍵スケジュールの強度の評価と捉える．用いる学習データは(最終段段鍵，秘密鍵) と(最終段鍵スケジュール内部状態，秘密鍵)の 2 種類とする．ニューラルネットワークはこのデータセットを学習することで，最終段の鍵データから秘密鍵の予測をする学習器となる．この学習器を作成することで, 漏洩してしまった最終段段鍵，もしくは最終段鍵スケジュール内部状態値から未知の秘密鍵をランダムではない精度で予測することが可能になる.

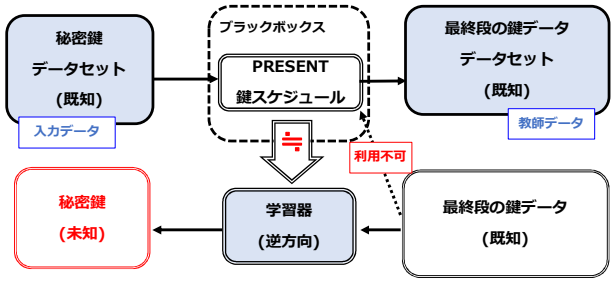

図 10 PRESENT の鍵スケジュール解析

5.2.2 実験 2 の手順

以下の①〜⑤の手順を 31 段 PRESENT に対して行った．なお, 学習データ数は 100000,10000,1000 の場合を試した.
①秘密鍵をデータ数だけランダムに定める.
②秘密鍵を鍵スケジュールに入力
③(最終段段鍵，秘密鍵)もしくは(最終段鍵スケジュール内部状態，秘密鍵)のデータセットを生成する.
なお，トレーニング・テストデータの分割は表 4 の通りである.

表 4 実験 2 のトレーニング・テストデータの分割

データセット数	トレーニング	テスト
100000	80000	20000
10000	8000	2000
1000	800	200

④トレーニングデータを用いてトレーニングを行う.
⑤テストデータを用いて各ビットの正答率 acc の平均を求める.

この①〜⑤の手順を全部で 3 回行い，全試行の acc の平均を最終的な値とする．この実験を行うことで，いかに少ないデータ数で最終段段鍵もしくは最終段鍵スケジュール内部状態から秘密鍵のランダムではない精度の予測ができるかを示す.

5.2.3 実験 2 の学習モデル

実験 2 のニューラルネットワークの構造，ハイパーパラメータは表 5 の通りである.

Vol.2021-DPS-186 No.67
Vol.2021-CSEC-92 No.67
2021/3/16

表 5　実験 2 の学習モデル

構造	入力層，中間層×3，出力層
パーセプトロン数	64or80-32-16-8-1
活性化関数	ReLU
損失関数	MSE(最小二乗誤差)
最適化関数	Adam
学習率	0.001
バッチサイズ	200
エポック数	300

5.2.4 実験 2 の結果

各ビットの平均の正答率は表 6,図 11 の通りである．

表 6　【実験 2】鍵スケジュール解析の結果

データ数	正答率 acc（入力:最終段鍵スケジュール内部状態）	正答率 acc（入力:最終段段鍵）
100000	0.998	0.890
10000	0.785	0.769
1000	0.560	0.558

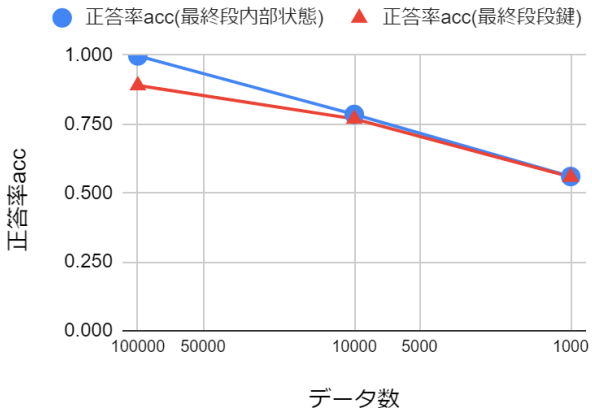

図 11　【実験 2】鍵スケジュール解析の結果

この結果より，データセット数が少なくなるほど正答率 acc も下がることが分かる．今回の実験ではいずれのパターンでも正答率は 0.5 を越え，ランダムでない精度の予測が実現した．つまり，多くとも 1000 組の(最終段段鍵，秘密鍵)および (最終段鍵スケジュール内部状態，秘密鍵)のデータセットがあれば最終段の鍵データから秘密鍵のランダムではない精度の予測が可能であると分かる．

6.　結論

本研究では軽量ブロック暗号 PRESENT に対してニューラルネットワークを用いた解析として 2 つの実験を行った．平文予測攻撃では 1200000 組の (暗号文, 平文)の組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ることにより，4 段まで暗号文から平文のランダムではない予測が可能となることを示した．

鍵スケジュール解析では多くとも 1000 組の(最終段段鍵，秘密鍵)，もしくは (最終段鍵スケジュール内部状態，秘密鍵)を学習させることにより，最終段の鍵データから秘密鍵のランダムではない予測が可能となることを示した．

参考文献

[1]Andrey Bogdanov et al. “PRESENT: An ultra-lightweight block cipher”. In: International workshop on cryptographic hardware and embedded systems. Springer. 2007, pp. 450–466.

[2]Manan Pareek et al. “Deep Learning based Analysis of the Key Scheduling Algorithm of PRESENT cipher” Cryptology ePrint Archive: Report 2020/981, 2020

[3]佐藤駿介，武田正之，松澤智史 “深層学習を用いた現代暗号の解読手法”.東京理科大学理工学研究科情報科学専攻修士論文(未公刊), 東京理科大学図書館, 2019

[4]電子情報通信学会 ”情報セキュリティハンドブック” ,2004 pp25-26

[5]金子敏信 “共通鍵暗号の安全性評価”，2013 https://www.jstage.jst.go.jp/article/essfr/7/1/7_14/_pdf