Wykorzystanie metod sztucznej inteligencji w analizie kanału bocznego: detekcja anomalii i klasyfikacja wzorców emisji elektromagnetycznej

Konrad Szczepankiewicz, Marian Wnuk
Wojskowa Akademia Techniczna, Instytut Systemów Łączności, ul. Gen. Sylwestra Kaliskiego 2, 00-908 Warszawa

Streszczenie: W artykule przedstawiono metodę dwustopniowej analizy emisji elektromagnetycznej generowanej przez mikrokontrolery realizujące operacje kryptograficzne, z wykorzystaniem technik sztucznej inteligencji. Pierwszy etap obejmuje detekcję anomalii w sygnale przy użyciu autoenkodera jednowymiarowego (1D AE), co umożliwia wyznaczenie fragmentów sygnału zawierających aktywność szyfrującą. Następnie, zidentyfikowane okna są klasyfikowane przy użyciu jednowymiarowej konwolucyjnej sieci neuronowej (1D CNN) w celu określenia, który algorytm szyfrowania był użyty. Podejście to pozwala na zwiększenie dokładności klasyfikacji i efektywność ekstrakcji informacji w kontekście ataków kanałem bocznym (Side Channel Analysis – SCA). Eksperymenty przeprowadzone na platformach STM32 i RP2040 potwierdzają skuteczność metody, wykazując, że połączenie autoenkodera i sieci CNN może stanowić wartościowe narzędzie do pasywnej analizy bezpieczeństwa sprzętowego.

Słowa kluczowe: konwolucyjne sieci neuronowe, sieci neuronowe, autoenkoder, kanał boczny, rozpoznawanie wzorców emisji

1. Wprowadzenie

Bezpieczeństwo układów wbudowanych staje się kluczowym zagadnieniem we współczesnych systemach elektronicznych, w szczególności w urządzeniach IoT oraz zastosowaniach kryptograficznych.

Jednym z istotnych zagrożeń dla integralności takich systemów są ataki kanałem bocznym SCA (ang. *Side Channel Attacks*), które polegają na pozyskiwaniu informacji na podstawie analizy fizycznych emisji generowanych przez urządzenia – w tym emisji elektromagnetycznej (EM). Emisje te mogą zawierać wzorce charakterystyczne dla konkretnych operacji kryptograficznych, a ich analiza umożliwia nie tylko rozpoznanie wykonywanego algorytmu szyfrującego, ale także w niektórych przypadkach ekstrakcję kluczy szyfrujących. Tradycyjne metody analizy takich sygnałów oparte są na przetwarzaniu sygnałów i statystyce, jednak mają one ograniczoną skuteczność w warunkach dużego szumu lub złożonych scenariuszy czasowych.

W artykule zaproponowano podejście dwustopniowe z wykorzystaniem metod głębokiego uczenia. W pierwszym etapie zastosowano autoenkoder jednowymiarowy (1D AE) w celu wykrycia fragmentów sygnału, w których występuje aktywność szyfrująca – na podstawie analizy rekonstrukcji sygnału i detekcji anomalii. Taka metoda pozwala automatycznie wyodrębnić interesujące okna czasowe bez konieczności stosowania ręcznej synchronizacji.

W drugim etapie wyodrębnione fragmenty są klasyfikowane przy pomocy jednowymiarowej konwolucyjnej sieci neuronowej (1D CNN), która rozpoznaje charakterystyczne cechy emisji związane z użyciem konkretnego algorytmu szyfrowania, takiego jak: AES-128, DES, 3DES, SM4, IDEA czy Blowfish. Połączenie tych dwóch modeli umożliwia zbudowanie systemu, który w sposób zautomatyzowany i skuteczny analizuje emisję EM w kontekście pasywnych ataków kanałem bocznym.

Autor korespondujący:
Konrad Szczepankiewicz, konrad.szczepankiewicz@wat.edu.pl

Artykuł recenzowany
nadesłany 07.08.2025 r., przyjęty do druku 30.09.2025 r.

2. Powiązane prace

Ataki kanałem bocznym stanowią istotne zagrożenie dla bezpieczeństwa systemów kryptograficznych, zwłaszcza w przypadku urządzeń wbudowanych. Tradycyjna analiza emisji elektromagnetycznej (EM) opiera się na metodach statystycznych i klasycznym przetwarzaniu sygnałów. Do najczęściej stosowanych technik należą różnicowa analiza mocy (DPA), różnicowa analiza emisji elektromagnetycznej (DEMA) oraz analiza korelacyjna (CPA) [1, 2]. Metody te wymagają jednak uprzedniego ręcznego wyodrębnienia fragmentów sygnału zawierających operacje kryptograficzne, co utrudnia ich automatyzację i zastosowanie w analizach masowych.

W ostatnich latach rośnie zainteresowanie wykorzystaniem metod sztucznej inteligencji w analizie kanałów bocznych.

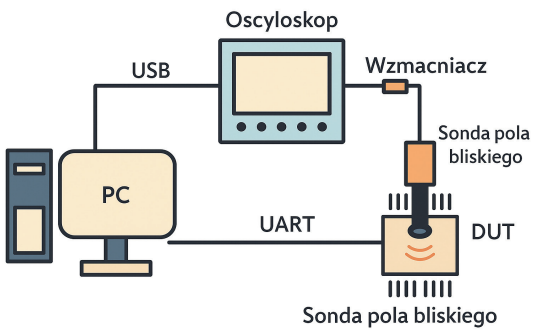
Badania [3, 4] wykazały, że sieci neuronowe, a zwłaszcza sieci konwolucyjne (CNN), mogą przewyższać podejścia klasyczne w zadaniach klasyfikacji sygnałów EM – szczególnie w warunkach zaszumienia lub braku precyzyjnej synchronizacji sygnału [5]. Pomimo wysokiej skuteczności CNN w rozpoznawaniu wzorców, rzadko spotyka się rozwiązania, które automatycznie identyfikują fragmenty sygnału zawierające aktywność szyfrującą. Zazwyczaj proces ten opiera się na ręcznej synchronizacji lub stosowaniu znaczników czasowych.

W artykule zaproponowano zintegrowane podejście łączące autoenkoder i konwolucyjną sieć neuronową. Autoenkoder służy do automatycznej detekcji anomalii i wyodrębniania okien czasowych zawierających operacje kryptograficzne, natomiast CNN dokonuje klasyfikacji typu użytego algorytmu szyfrującego. Taka kombinacja metod umożliwia zwiększenie autonomii i dokładności analizy SCA, otwierając drogę do bardziej efektywnych systemów monitorowania bezpieczeństwa sprzętowego.

3. Stanowisko pomiarowe

Pomiar emisji elektromagnetycznej został przeprowadzony na dwóch platformach sprzętowych: STM32L476RG oraz RP2040. Oba mikrokontrolery zostały wybrane ze względu na swoją popularność w systemach wbudowanych oraz możliwość implementacji szyfrów w sposób programowy.

Każdy mikrokontroler był zaprogramowany do wykonywania operacji szyfrowania blokowego z użyciem sześciu algorytmów: AES, DES, 3DES, SM4, IDEA oraz Blowfish. Dodatkowo zarejestrowano klasę sygnałów tła (szum). W przypadku AES zastosowano klucz 128-bitowy, natomiast pozostałe algorytmy realizowano w standardowych parametrach implementacyjnych (tryb ECB). Nie rozważano innych algorytmów szyfrujących.



Rys. 1. Schemat stanowiska pomiarowego
Fig. 1. Measurement setup diagram

W celu przechwytywania emisji EM zastosowano sondę bliskiego pola umieszczoną możliwie blisko układu scalonego. Zastosowano również wzmacniacz niskoszumowy (LNA). Do rejestracji sygnałów użyto cyfrowego oscyloskopu (Picoscope 3206D).

Tabela 1. Wykaz elementów stanowiska pomiarowego
Table 1. List of components of the measurement setup

Element	Model
Oscyloskop	Picoscope 3206D
Sonda	Riscure EM probe (ø1,25mm)
Wzmacniacz (LNA)	Wzmacniacz stanowi zintegrowaną część wykorzystanej sondy firmy Riscure
Badane układy (DUT)	STM32L476RG, RP2040

Komputer klasy PC pełnił funkcję jednostki sterującej – wysyłał dane wejściowe (plaintext) przez port szeregowy do mikrokontrolera i rejestrował przebiegi z oscyloskopu. Dodatkowo komputer służył do dalszego przetwarzania i analizy zarejestrowanych danych.

Schemat stanowiska pomiarowego przedstawiono na rys. 1. W tabeli 1. zamieszczono wykaz zastosowanych na stanowisku pomiarowym komponentów.

4. Zbiór danych

Dla każdego z algorytmów kryptograficznych i dla obu mikrokontrolerów (STM32L476RG i RP2040) zarejestrowano po 600 przebiegów czasowych zawierających operację szyfrowania.

Zebrane dane zapisano w formie jednowymiarowych sygnałów czasowych, zorganizowanych w katalogi odpowiadające poszczególnym algorytmom szyfrowania. Każdy przebieg został znormalizowany do zakresu [–1, 1] oraz przepróbkowany do długości 128 000 próbek, co zapewniło spójność wejścia modeli. Zbiór danych został podzielony na część treningową (70 %), walidacyjną (10 %) oraz testową (15 %), przy zachowaniu równowagi liczby przykładów dla każdej klasy.

Zastosowano techniki augmentacji danych: przesunięcia w czasie, losowe skalowanie amplitudy oraz dodanie białego szumu Gaussowskiego.

Tak przygotowany zbiór danych sygnałów posłużył zarówno do nauki autoenkodera do detekcji anomalii, jak i do treningu konwolucyjnej sieci neuronowej (CNN) do klasyfikacji typu algorytmu szyfrującego.

5. Architektura modelu analitycznego

Zaproponowana metoda analizy sygnałów kanału bocznego składa się z dwóch głównych etapów: detekcji istotnych fragmentów czasowych oraz klasyfikacji typu algorytmu szyfrującego. Każdy z tych etapów realizowany jest przez odrębny model sieci neuronowej, tworząc spójną architekturę przetwarzania sygnałów elektromagnetycznych.

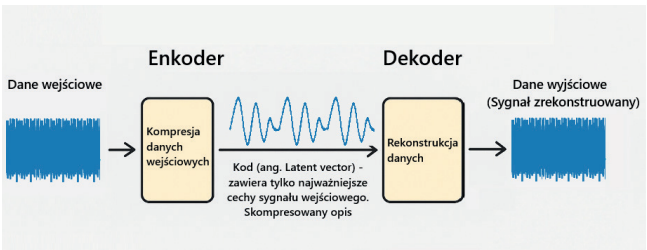
Pierwszym komponentem systemu jest autoenkoder, którego zadaniem jest automatyczne wykrywanie fragmentów sygnału zawierających aktywność kryptograficzną. Tradycyjne podejścia do analizy SCA często opierają się na ręcznym wycinaniu sygnałów w oparciu o synchronizację lub znaczniki czasowe. W proponowanej metodzie etap ten został zastąpiony uczeniem nienadzorowanym, które pozwala zidentyfikować anomalie w przebiegach EM – związane z momentami wykonywania operacji szyfrowania – bez konieczności wcześniejszej wiedzy o strukturze sygnału. Autoenkoder uczony jest na „nieaktywnych" fragmentach sygnału (pozbawionych operacji kryptograficznych), a następnie stosowany do rekonstrukcji całych przebiegów. Miejsca o wysokim błędzie rekonstrukcji są interpretowane jako potencjalne obszary aktywności i poddawane dalszej analizie (okna czasowe do dalszej klasyfikacji przez sieć konwolucyjną).

Drugim komponentem systemu jest konwolucyjna sieć neuronowa, której celem jest klasyfikacja typu algorytmu szyfrującego na podstawie wcześniej wyodrębnionych przez autoenkoder fragmentach przebiegu emisji EM.

Sieci CNN wykazują wysoką skuteczność w zadaniach przetwarzania sygnałów 1D, dzięki zdolności do automatycznego wykrywania istotnych cech reprezentatywnych dla danej klasy. W proponowanym rozwiązaniu CNN analizuje wyłącznie te okna czasowe, które zostały uznane przez autoenkoder za potencjalnie istotne, co zwiększa trafność klasyfikacji i pozwala pominąć duże fragmenty danych nieistotnych z punktu widzenia bezpieczeństwa.

6. Detekcja wyróżniających się wzorców sygnałowych

W ramach etapu detekcji wykorzystano autoenkoder 1D o architekturze enkoder–dekoder. Enkoder zawiera warstwy konwolucyjne z funkcją aktywacji ReLU (ang. *Rectified Linear Unit*), która przepuszcza tylko wartości dodatnie sygnału, wprowadzając nieliniowość i umożliwiając wychwycenie skomplikowanych zależności w danych. Dodatkowo zastosowano warstwy pooling (warstwy podpróbkowania), które zmniejszają wymiar sygnału, wyodrębniają najistotniejsze cechy i zwiększają odporność modelu na niewielkie zakłócenia. Dekoder opiera się na warstwach dekonwolucyjnych (ang. *transposed convolution*), które przywracają sygnał do pierwotnej długości, a końcowa warstwa ogranicza wartości do przedziału [–1, 1].



Rys. 2. Schemat autoenkodera
Fig. 2. Autoencoder diagram

Model autoenkodera był trenowany wyłącznie na fragmentach pozbawionych aktywności kryptograficznej, co pozwoliło mu wiernie odtwarzać przebiegi typowe dla pracy „spoczynkowej" mikrokontrolera. Anomalie są identyfikowane na podstawie błędu rekonstrukcji: jako próg przyjęto średnią + 2 × odchylenie standardowe błędu na zbiorze walidacyjnym. Analiza prowadzona jest w oknach 1024 próbek, przesuwanych co 256 próbek, a zdarzenie uznaje się za potencjalną operację kryptograficzną, jeśli obejmuje co najmniej kilka kolejnych okien (> 4096 próbek).

W ten sposób autoenkoder pełni funkcję modułu wstępnej detekcji, przekazując do CNN jedynie te fragmenty sygnału, które zawierają potencjalnie istotne wzorce emisji elektromagnetycznej.

7. Klasyfikacja wyróżniających się wzorców sygnałowych

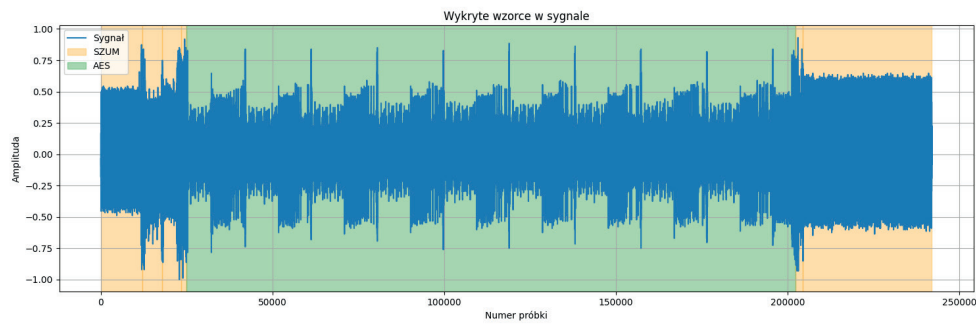
Do klasyfikacji, z jakiego algorytmu szyfrowania pochodzi dany fragment sygnału, wykorzystano jednowymiarową konwolucyjną sieć neuronową (1D CNN) [19]. Sieć ta została zaprojektowana w celu rozpoznawania typu algorytmu szyfrującego — AES-128, DES, 3DES, SM4, IDEA, Blowfish — oraz odróżniania ich od fragmentów szumu, na podstawie fragmentów sygnału wskazanych przez autoenkoder jako najbardziej informatywne.

Zastosowana architektura CNN składa się z trzech kolejnych warstw konwolucyjnych [20], w których liczba filtrów wzrasta wraz z głębokością sieci (odpowiednio 32, 64 i 128 filtrów), a długości filtrów maleją (7, 5, 3), co umożliwia wychwytywanie zarówno długoterminowych, jak i krótkoterminowych zależności w sygnale. Po każdej warstwie konwolucyjnej stosowana jest funkcja aktywacji ReLU oraz warstwa pooling [21], co redukuje wymiary danych i wprowadza translacyjną odporność na przesunięcia w czasie sygnału. Na końcu części konwolucyjnej zastosowano warstwę uśredniania adaptacyjnego, pozwalającą na standaryzację długości wyjściowych reprezentacji niezależnie od rozmiaru wejściowych fragmentów sygnału.

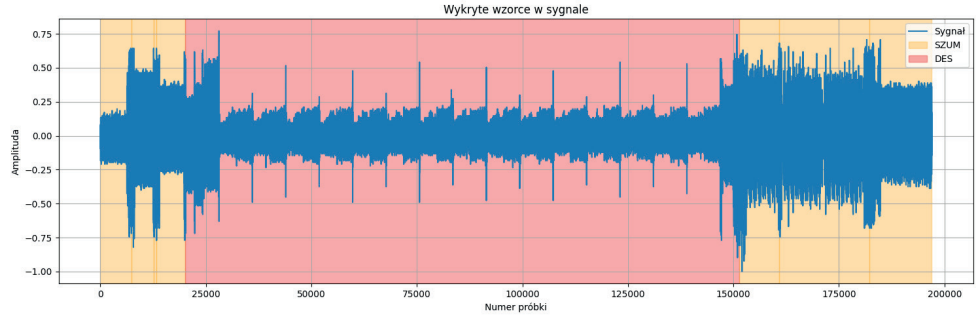
Część klasyfikacyjna sieci obejmuje liniową warstwę redukującą wymiar z 128 do 64 neuronów, po której zastosowano funkcję aktywacji ReLU oraz warstwę dropout ($p = 0{,}3$) w celu ograniczenia przeuczenia. Na końcu znajduje się warstwa wyjściowa dopasowana do siedmiu klas odpowiadających poszczególnym algorytmom szyfrowania oraz szumowi.

Trening sieci przeprowadzono z użyciem optymalizatora Adam (*learning rate* = 0,001, *betas* = (0,9, 0,999)) przy *batch size* = 32, a funkcją kosztu była entropia krzyżowa (ang. *cross-entropy*) dla problemu klasyfikacji wieloklasowej. Model trenowano przez 50 epok z mechanizmem *early stopping* monitorującym brak poprawy przez pięć kolejnych epok, co pozwoliło uniknąć nadmiernego dopasowania do danych treningowych.

Tak zaprojektowana architektura umożliwia automatyczne wyodrębnianie najbardziej istotnych fragmentów sygnału z punktu widzenia rozróżnienia algorytmów szyfrujących oraz ich skuteczną klasyfikację, jednocześnie eliminując znaczną



Rys. 3. Sygnał emisji z nałożonymi oznaczeniami (kolor żółty – szum, zielony – AES)
Fig. 3. Emission signal with annotations (Yellow – noise, Green – AES)



Rys. 4. Sygnał emisji z nałożonymi oznaczeniami (kolor żółty – szum, czerwony – DES)
Fig. 4. Emission signal with annotations (Yellow – noise, Red – DES)

Tabela 2. Dokładność klasyfikacji CNN dla poszczególnych algorytmów szyfrowania
Table 2. CNN classification accuracy for individual encryption algorithms

Algorytm	Dokładność klasyfikacji [%]
AES	96,7
DES	95,4
3DES	95,9
SM4	91,4
IDEA	81,1
Blowfish	82,7
Szum	92,6
Średnia	90,82

część danych nieistotnych, co zwiększa efektywność analizy i pozwala na bardziej precyzyjne wnioski w kontekście bezpieczeństwa kryptograficznego. Cały model został zaimplementowany z wykorzystaniem biblioteki PyTorch.

8. Wyniki

Opracowany system analizy sygnałów elektromagnetycznych został przetestowany na rzeczywistych danych pomiarowych, obejmujących różne klasy operacji szyfrowania blokowego. Zastosowanie autoenkodera pozwoliło na skuteczne wykrywanie fragmentów sygnału zawierających struktury nietypowe lub odbiegające od wzorca – co umożliwiło wyodrębnienie istotnych okien czasowych do dalszej analizy. Na tej podstawie klasyfikator CNN dokonywał przypisania każdego z wykrytych segmentów do jednej z zadanych klas (AES-128, DES, 3DES, SM4, IDEA, Blowfish, szum). System osiągnął wysoką skuteczność klasyfikacji, przekraczając 90 % dokładności na zestawie testowym.

Wprowadzenie etapu detekcji anomalii pozwoliło znacząco ograniczyć liczbę fałszywych klasyfikacji, eliminując fragmenty tła lub zakłóceń z dalszego przetwarzania. W praktyce przyczyniło się to do poprawy stabilności i interpretowalności wyników końcowych. Ponadto model wykazywał odporność na niewielkie zakłócenia pomiarowe i różnice w długości sygnału, co potwierdza jego użyteczność w warunkach rzeczywistych.

Wynikiem działania całego systemu analitycznego był oryginalny sygnał emisji elektromagnetycznej z nałożonymi oznaczeniami czasowymi. Fragmenty zidentyfikowane jako zawierające operacje szyfrowania zostały wyróżnione kolorystycznie – każda klasa operacji była reprezentowana przez inny kolor, co pozwalało intuicyjnie wskazać, w którym miejscu sygnału wystąpiła konkretna aktywność kryptograficzna.

W analogiczny sposób system wizualizuje przebiegi z zaznaczonymi fragmentami emisji odpowiadającymi pozostałym zaimplementowanym algorytmom szyfrowania, tj. 3DES, SM4, IDEA oraz Blowfish.

Najwyższą skuteczność klasyfikacji uzyskano dla klas AES, DES/3DES, SM4 oraz dla klasy „szum". Największe trudności sprawiała natomiast poprawna identyfikacja sygnałów pochodzących z algorytmów Blowfish i IDEA, co może wynikać z faktu, że przebiegi emisji generowane przez te algorytmy zawierają najmniej unikalnych cech charakterystycznych, pozwalających na ich jednoznaczne odróżnienie od pozostałych klas. Weryfikację przeprowadzono poprzez analizę map cech CNN (ang. *feature maps*) – warstwy konwolucyjne wydobywały mniej zróżnicowanych aktywacji dla tych klas niż dla AES czy DES. Ewentualnym usprawnieniem w tej kwestii może być rozszerzenie CNN o kolejne warstwy lub zastosowanie hybrydowej architektury (CNN+LSTM). LSTM to sieć rekurencyjna do przechowywania informacji w czasie (ang. *Long Short-Term Memory*).

9. Wnioski

W artykule zaprezentowano zintegrowane podejście do analizy sygnałów elektromagnetycznych w kontekście ataków kanałem bocznym, oparte na wykorzystaniu metod sztucznej inteligencji. Proponowana architektura, składająca się z autoenkodera i konwolucyjnej sieci neuronowej, umożliwia skuteczną i w pełni automatyczną detekcję oraz klasyfikację aktywności kryptograficznej w sygnałach generowanych przez mikrokontrolery.

Zastosowanie autoenkodera pozwoliło wyeliminować ręczną synchronizację sygnału oraz efektywne wyodrębnienie istotnych fragmentów czasowych. Klasyfikator CNN z powodzeniem przypisywał wykryte okna do odpowiednich klas algorytmów szyfrujących, osiągając wysoką skuteczność (powyżej 90 % na zestawie testowym), nawet w warunkach umiarkowanego zakłócenia i przy zmiennej długości sygnału.

Opracowany system wykazał się dużą odpornością na szum oraz potencjałem do zastosowań praktycznych, np. w pasywnych systemach monitorowania bezpieczeństwa sprzętowego. Dodatkowo metoda charakteryzuje się dobrą skalowalnością i może zostać rozszerzona o nowe klasy algorytmów lub zaadaptowana do innych typów kanałów bocznych (np. analizy poboru mocy).

W dalszych pracach planuje się:
- zwiększenie rozdzielczości czasowej lokalizacji zdarzeń,
- dostosowanie architektury do pracy w czasie rzeczywistym,
- rozszerzenie zbioru danych o inne typy operacji i platformy sprzętowe,
- badanie innych kanałów bocznych (np. pobór prądu).

Zaproponowane rozwiązanie stanowi krok w kierunku bardziej autonomicznych, precyzyjnych i adaptacyjnych narzędzi do analizy bezpieczeństwa układów elektronicznych z wykorzystaniem nowoczesnych metod głębokiego uczenia.

Bibliografia

1. Kocher P., Jaffe J., Jun B., *Differential Power Analysis*, Advances in Cryptology — CRYPTO, Vol. 1666, No. 25, 1999, 388–397, DOI: 10.1007/3-540-48405-1_25.
2. Mangard S., Oswald E., Popp T., *Power Analysis Attacks*, Springer US, 2007, DOI: 10.1007/978-0-387-38162-6.
3. Zaid G., Bossuet L., Habrard A., Venelli A., *Methodology for Efficient CNN Architectures in Profiling Attacks*, "IACR Transactions on Cryptographic Hardware and Embedded Systems", Vol. 2020, No. 1, 2019, 1-36, DOI: 10.13154/tches.v2020.i1.1-36.
4. Ahmed A.A., Hasan M.K., Aman A.H., Abdulkadir R.A., Islam S., Farhan B.A., *Efficient Convolutional Neural Network Based Side Channel Attacks Based on AES Cryptography*, IEEE Student Conf. Research and Development (SCOReD), No. 12, 2023, 144–149, DOI: 10.1109/SCOReD60679.2023.10563332.
5. Maghrebi H., Portigliatti T., Prouff E., *Breaking Cryptographic Implementations Using Deep Learning Techniques*, Security, Privacy, and Applied Cryptography Engineering, Vol. 10076, No. 1, 2016, 3–26, DOI: 10.1007/978-3-319-49445-6_1.
6. Jin M., Zheng M., Hu H., Yu N., *An Enhanced Convolutional Neural Network in Side-Channel Attacks and Visual-*

ization, Proceedings of 2020 the 10th International Workshop on Computer Science and Engineering (WCSE 2020), 2020, 30–36, DOI: 10.18178/wcse.2020.06.006.
7. Wang H., Luo Y., Long F., Fu Y., *Anomalous Radio Signal Detection Based on an Adversarial Autoencoder*, "Electronics", Vol. 14, No. 9, 2025, DOI: 10.3390/electronics14091785.
8. Li L., Yan J., Wang H., Jin Y., *Anomaly Detection of Time Series with Smoothness-Inducing Sequential Variational Auto-Encoder*, "IEEE Transactions on Neural Networks and Learning Systems", Vol. 32, No. 3, 2021, 1177–1191, DOI: 10.1109/TNNLS.2020.2980749.
9. Chen Z., Zhou Y., *Dual-Rail Random Switching Logic: A Countermeasure to Reduce Side Channel Leakage*, Cryptographic Hardware and Embedded Systems – CHES 2006, Vol. 4249, No. 20, 2006, 242–254, DOI: 10.1007/11894063_20.
10. Wang R., Wang H., Dubrova E., *Far Field EM Side-Channel Attack on AES Using Deep Learning*, ACM Workshop on Attacks and Solutions in Hardware Security, 2020, 35–44, DOI: 10.1145/3411504.3421214.
11. Gong D., Liu L., Le V., Saha B., Mansour M.R., Venkatesh S., Van Den Hengel A., *Memorizing Normality to Detect Anomaly: Memory-augmented Deep Autoencoder for Unsupervised Anomaly Detection*, 2019 IEEE/CVF International Conference on Computer Vision (ICCV), 2019, 1705–1714, DOI: 10.1109/ICCV.2019.00179.
12. Feng H., Lin W., Shang W., Cao J., Huang W., *MLP and CNN-based Classification of Points of Interest in Side-channel Attacks*, "International Journal of Networked and Distributed Computing", Vol. 8, No. 2, 2020, 108–117, DOI: 10.2991/ijndc.k.200326.001.pdf.
13. Liu W., Zhang Y., Chen Y., Wang Q., *Side-Channel Profiling Attack Based on CNNs' Backbone Structure Variant*, "Electronics", Vol. 14, No. 10, 2025, DOI: 10.3390/electronics14102006.
14. Zhang Y., Chen Y., Wang J., Pan Z., *Unsupervised Deep Anomaly Detection for Multi-Sensor Time-Series Signals*, "IEEE Transactions on Knowledge and Data Engineering", Vol. 35, No. 2, 2023, 2118–2132, DOI: 10.1109/TKDE.2021.3102110.
15. Zhang C., Li S., Zhang H., Chen Y., *VELC: A New Variational AutoEncoder Based Model for Time Series Anomaly Detection*, "International Journal of Machine Learning and Cybernetics", Vol. 14, 2022, 683–696, DOI: 10.1007/s13042-022-01657-w.
16. Szczepankiewicz K., Wnuk M., *Embedded Systems and their Vulnerabilities to Hardware Attacks*, "Biuletyn WAT", Vol. 72, No. 1, 2023, 59–68, DOI: 10.5604/01.3001.0054.2897.
17. Szczepankiewicz K., Wnuk M., *Recognition of block cipher algorithms based on radiated emission*, 2024 International Symposium on Electromagnetic Compatibility – EMC Europe, No. 9, 2024, 475–478, DOI: 10.1109/EMCEurope59828.2024.10722119.
18. Lemarchand F., Marlin C., Montreuil F., Nogues E., Pelcat M., *Electro-Magnetic Side-Channel Attack Through Learned Denoising and Classification*, 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), No. 5, 2020, 2882–2886, DOI: 10.1109/ICASSP40776.2020.9053913.
19. Kiranyaz S., Avci O., Abdeljaber O., Ince T., Gabbouj M., Inman D.J., *1D convolutional neural networks and applications: A survey*, "Mechanical Systems and Signal Processing", Vol. 151, 2021, DOI: 10.1016/j.ymssp.2020.107398.
20. Cordeiro J.R., Raimundo A., Postolache O., Sebastião P., *Neural Architecture Search for 1D CNNs—Different Approaches Tests and Measurements*, "Sensors", Vol. 21, No. 23, 2021, DOI: 10.3390/s21237990.
21. Zhao X., Wang L., Zhang Y., Han X., Deveci M., Parmar M., *A review of convolutional neural networks in computer vision*, "Artificial Intelligence Review", Vol. 57, No. 4, DOI: 10.1007/s10462-024-10721-6.

Application of Artificial Intelligence Methods in Side-Channel Analysis: Anomaly Detection and Classification of Electromagnetic Emission Patterns

Abstract: This article presents a two-stage method for analyzing electromagnetic emissions generated by microcontrollers performing cryptographic operations, utilizing artificial intelligence techniques. The first stage involves anomaly detection in the signal using a one-dimensional autoencoder (1D AE), enabling the identification of signal segments containing cryptographic activity. Subsequently, the identified windows are classified using a one-dimensional convolutional neural network (1D CNN) to determine which encryption algorithm was used. This approach enhances classification accuracy and improves information extraction efficiency in the context of side-channel analysis (SCA) attacks. Experiments conducted on STM32 and RP2040 platforms confirm the effectiveness of the method, demonstrating that the combination of an autoencoder and CNN can serve as a valuable tool for passive hardware security analysis.

Keywords: convolutional neural networks, neural networks, autoencoder, side channel, emission pattern recognition

mgr inż. Konrad Szczepankiewicz

konrad.szczepankiewicz@wat.edu.pl
ORCID: 0000-0003-3292-8113

Ukończył studia na Wydziale Elektroniki Wojskowej Akademii Technicznej, gdzie w 2021 r. obronił pracę magisterską. Od 2022 r. jest doktorantem w Szkole Doktorskiej Wojskowej Akademii Technicznej oraz członkiem Zespołu Anten Inteligentnych i Propagacji Fal na Wydziale Elektroniki WAT, kierowanym przez prof. dr. hab. inż. Mariana Wnuka. Jego działalność naukowa koncentruje się na badaniach emisji ujawniającej urządzeń elektronicznych oraz analizie zagrożeń związanych z ulotem informacji kanałami bocznymi. Prowadzone prace obejmują zarówno detekcję i analizę sygnałów emitowanych przez układy elektroniczne, jak i opracowanie metod ich klasyfikacji oraz oceny potencjalnych zagrożeń bezpieczeństwa informacyjnego. Szczególną uwagę poświęca wykorzystaniu metod sztucznej inteligencji i technik uczenia maszynowego do identyfikacji wzorców emisji i wykrywania anomalii w kontekście ochrony systemów teleinformatycznych.

prof. dr hab. inż. Marian Wnuk

marian.wnuk@wat.edu.pl
ORCID: 0000-0003-4576-4023

Studiował systemy pomiarowe na Politechnice Warszawskiej, gdzie uzyskał tytuł magistra inżyniera. Po ukończeniu studiów rozpoczął pracę w ZZEAP ELPO jako konstruktor. Następnie został powołany do zawodowej służby wojskowej i skierowany do Wojskowej Akademii Technicznej, gdzie nieprzerwanie pracował jako starszy asystent, później kierownik laboratorium i wykładowca, a od maja 1989 r. jako adiunkt – początkowo w Instytucie Układów Elektronicznych, a po reorganizacji Wydziału Elektroniki – w Instytucie Telekomunikacji. W 1987 r. obronił rozprawę doktorską na Wydziale Elektroniki Wojskowej Akademii Technicznej. Stopień doktora habilitowanego uzyskał w 1999 r.; rozprawa habilitacyjna otrzymała III nagrodę Rektora Wojskowej Akademii Technicznej w konkursie na najlepszą pracę habilitacyjną. Tytuł profesora został mu nadany w 2006 r.

Jest członkiem IEEE oraz Electromagnetic Academy w MIT. Należy do wielu rad naukowych z dziedziny elektroniki, telekomunikacji, a także instytutów badawczo-przemysłowych, jak również do trzech sekcji Komitetu PAN, w tym Sekcji Kompatybilności Elektromagnetycznej, gdzie pełni funkcję wiceprzewodniczącego.

Specjalizuje się w problematyce analizy pola antenowego oraz konstrukcji anten na warstwach dielektrycznych, a także w zagadnieniach kompatybilności elektromagnetycznej systemów łączności. Opublikował ponad 450 prac dotyczących anten, propagacji fal elektromagnetycznych i kompatybilności elektromagnetycznej. Kieruje zespołem prowadzącym badania naukowe i prace rozwojowe. Otrzymał nagrody Ministra Obrony Narodowej za wybitne osiągnięcia naukowe i praktyczne zastosowanie ich wyników. Pełnił również funkcję dziekana Wydziału Elektroniki.