SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

DIPLOMSKI RAD br. 1966

Optimizirane izlazne funkcije klasifikatora temeljenog na umjetnim neuronskim mrežama u domeni implementacijskih napada na kriptografske uređaje

Juraj Fulir

Zagreb, travanj 2019.

Umjesto ove stranice umetnite izvornik Vašeg rada.
Da bi ste uklonili ovu stranicu obrišite naredbu `\izvornik`.

ZAHVALA'n'STUFF

SADRŽAJ

1. Uvod **1**

2. Implementacijski napadi na kriptografske uređaje **2**
2.1. Side-channel napadi 2
2.2. Izvedba napada 2
2.3. DPA skupovi podataka 2

3. Klasifikator temeljen na umjetnim neuronskim mrežama **3**
3.1. Umjetne neuronske mreže 3
3.2. Izlazne funkcije 3

4. Optimizacija simboličkom regresijom (tehnički genetskim programiranjem...) **4**
4.1. Simbolička regresija 4
4.2. Taboo evolucijski algoritam 4
4.3. Korišteni čvorovi i operatori 4

5. Implementacija **5**

6. Rezultati **6**
6.1. 9class 6
6.1.1. Uobičajene izlazne funkcije 6
6.1.2. Utjecaj parametra veličine taboo liste 6
6.2. 256class 6
6.2.1. Uobičajene izlazne funkcije 6
6.2.2. Utjecaj parametra veličine taboo liste 6

7. Buduća istraživanja **7**

8. Zaključak **8**

Literatura **9**

1. Uvod

Opis problema

2. Implementacijski napadi na kriptografske uređaje

2.1. Side-channel napadi

Postoji nekoliko vrsta.

Ovdje se obrađuje DPA.

2.2. Izvedba napada

Uštekaj uređaj, osciloskop na to i to mjesto i snimaj

Provjeri mogućnosti i zaključi najvjerojatniju

Problem netraktabilnosti postupka -> neuralke <3

2.3. DPA skupovi podataka

Ima HW i ovaj pravi

Nabaci i PCA redukcije i statistike iz jn

Mjere dobrote klasifikacije

Ne zaboravi referencu na stranicu!

3. Klasifikator temeljen na umjetnim neuronskim mrežama

3.1. Umjetne neuronske mreže

Svojstva kompresije i generalizacije

Problem odabira arhitekture, hiperparametara i optimizacije

3.2. Izlazne funkcije

Nomenklatura izlazne/prijenosne fje (ona 2 cool rada)

Bitka za odabir akrivacijske fje (nađi onaj rad di pljuje po sigmoidi i relu (elu rad?))

4. Optimizacija simboličkom regresijom (tehnički genetskim programiranjem...)

4.1. Simbolička regresija

Opis i svojstva SR

Utjecaj i brojnost parametara u GA (moš linkat i svoj završni rad :P)

4.2. Taboo evolucijski algoritam

Problem konvergencije i stohastičnosti GP-a

EA oplemenjen taboo listom iz algoritma Taboo pretraživanja

4.3. Korišteni čvorovi i operatori

Popis čvorova

Popis operatora (un/bin)

5. Implementacija

???

6. Rezultati

6.1. 9class

6.1.1. Uobičajene izlazne funkcije

Opis postupka pretrage

Tablica

Komentar

6.1.2. Utjecaj parametra veličine taboo liste

Tablica

Komentar

6.2. 256class

6.2.1. Uobičajene izlazne funkcije

Opis postupka pretrage

Tablica

Komentar

6.2.2. Utjecaj parametra veličine taboo liste

Tablica

Komentar

7. Buduća istraživanja

Primjena CNN na vremenskim uzorcima po uzoru na onaj rad

- Ispitivanje učinkovitosti korištene optimizacije na ostalim problemima
- Paralelna evolucija arhitekture i aktivacijskih fja

8. Zaključak

Radi/Ne radi.

Pronađene zanimljivosti.

Pouka za doma.

LITERATURA

Optimizirane izlazne funkcije klasifikatora temeljenog na umjetnim neuronskim mrežama u domeni implementacijskih napada na kriptografske uređaje

Sažetak

Proučiti postojeće metode u izgradnji izlaznih funkcija u umjetnim neuronskim mrežama. Posebnu pažnju posvetiti evolucijskim algoritmima simboličke regresije za izgradnju ciljanih funkcija. Ustanoviti moguće nedostatke postojećih algoritama ili mogućnost poboljšanja. Primijeniti evoluirane izlazne funkcije u homogenoj ili heterogenoj umjetnoj neuronskoj mreži na skupovima DPAv2 i DPAv4 te odrediti mjere kvalitete izgrađenog klasifikatora: točnost, preciznost, odziv te F mjere. Usporediti učinkovitost ostvarenih postupaka s postojećim rješenjima iz literature. Radu priložiti izvorne tekstove programa, dobivene rezultate uz potrebna objašnjenja i korištenu literaturu.

Ključne riječi: Ključne riječi, odvojene zarezima.

Title

Abstract

Abstract.

Keywords: Keywords.