

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

Juraj Fulir



Sveučilište u Zagrebu

Fakultet elektrotehnike i računarstva

Zavod za elektroniku, mikroelektroniku, računalne i inteligentne sustave

*Mentor: prof. dr. sc. Domagoj Jakobović,  
Karlo Knežević, mag. ing. comp.*

**DIPLOMSKI RAD**

## 1 Uvod

## 2 Implementacijski napadi

- Napad analizom potrošnje električne energije
- Podatkovni skupovi

## 3 Odabir arhitekture

- Rezultati DPAv4 (oktet)
- Rezultati DPAv4 (HW)

## 4 Izgradnja aktivacijskih funkcija

- Rezultati DPAv4 (oktet)
- Rezultati DPAv4 (HW)

## 5 Zaključak

- Kriptografski uređaji su nezamjenjiv element digitalne infrastrukture modernog društva
- Pametne kartice (bankovne kartice, identifikacijski dokumenti)
- Kriptoalgoritam štiti povjerljive podatke
- Dobar kriptoalgoritam je siguran, no sklopovlje emitira informacije u okoliš

- Pretpostavka: emitirane informacije i sadržaj registara su korelirani
- Cilj: otkriti tajni ključ na temelju izmjerenih emisija (razlučitelj)
- Uvjeti: uređaj mora biti uključen i mora sadržavati tajni ključ
- Postoji više vrsta: aktivni i pasivni

- Ideja: iskoristiti korelaciju između potrošnje el. energije uređaja i podataka zapisanih na uređaju
- Napad koji je iznimno teško detektirati
- Postoji više pristupa, među najpoznatijim je DPA

- Napad na AES-128
- Ulaz: trag potrošnje el. energije, proban Pearsonovim koeficijentima
- DPAv2: FPGA implementacija
- DPAv4: programska implementacija
- predikcija vrijednosti okteta ili Hammingove težine

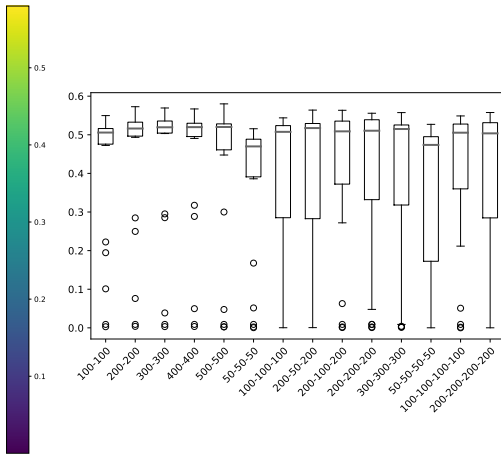
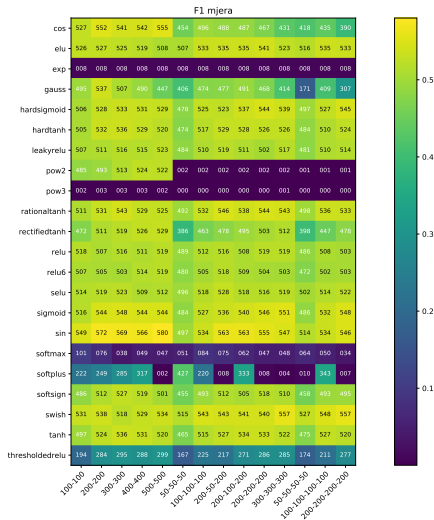
## Neuronska mreža

- Arhitektura: potpuno povezana, relativno plitka (do 4 skrivena sloja)
- Optimizacija: Adam, smanjivanje stope učenja, rano zaustavljanje
- Regularizacija: L2, normalizacija grupom

## Pretraga po rešetki

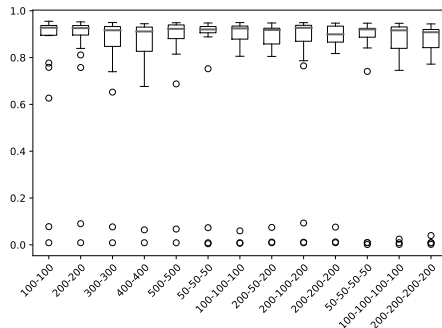
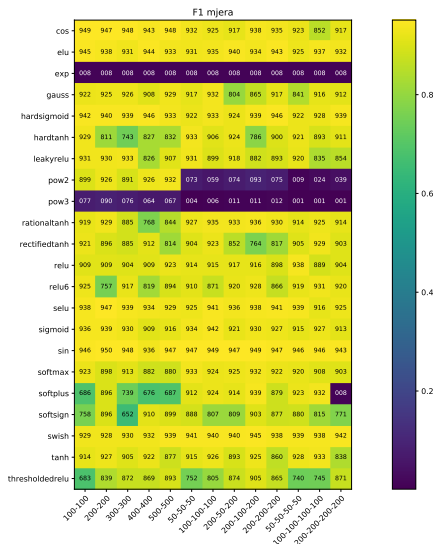
- Optimizacija stope učenja i L2 koeficijenta
- Usporedba arhitektura i aktivacijskih funkcija
- Odabir arhitektura, optimalnih za većinu funkcija

# Rezultati DPAv4 (oktet)





# Rezultati DPAv4 (HW)



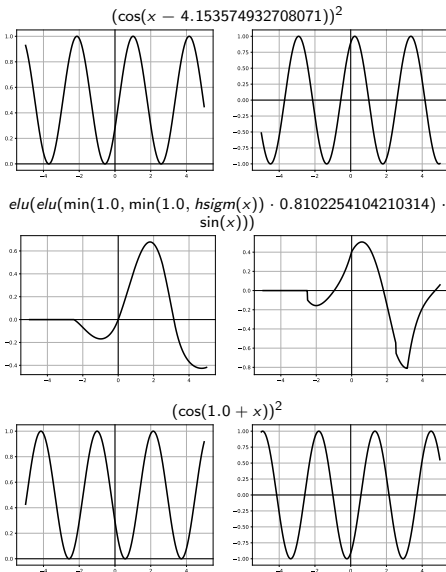
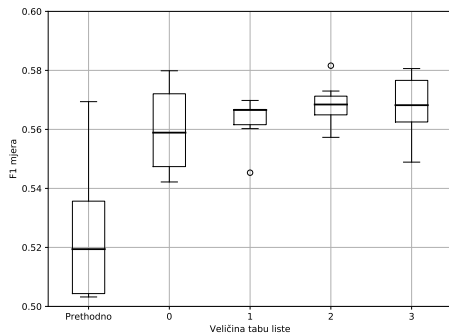
## Genetsko programiranje

- Populacijski algoritam
- Tabu lista
- Paralelna evaluacija

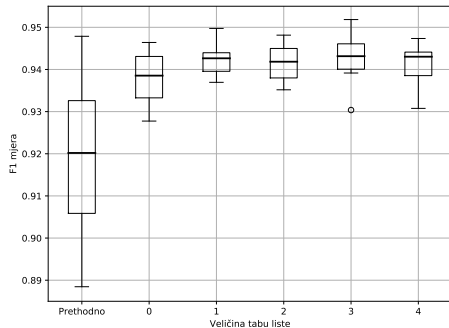
## Evolucija aktivacijske funkcije

- AF kao simboličko stablo
- Čvorovi: ulaz, konstanta, matematičke op. i popularne AF
- Po nekoliko operatora križanja i mutacije

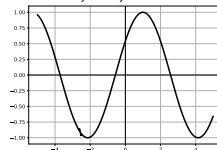
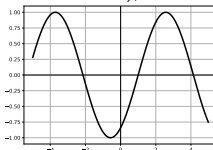
# Rezultati DPAv4 (oktet)



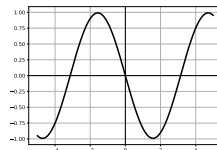
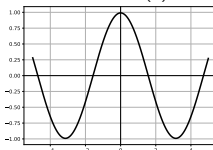
# Rezultati DPAv4 (HW)



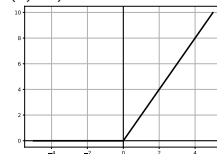
$$\sin(\min(\sin(\min(x, 0.5068783911631836) + 1.0), -0.9990098031722499) + x)$$



$$\cos(x) \cdot 0.9910098031767487$$



$$\text{ReLU}(\text{abs}(x) \cdot x)$$



- Sklopovlje je i dalje relativno sigurno
- Odabir AF ima utjecaj na performanse mreže
- Utjecaj AF može biti nepredvidiv
- Tabu lista pokazuje znakove poboljšanja

Otvorena pitanja za budući rad:

- Zašto su pronađene AF dobre (distribucija ulaza, kvaliteta gradijenta)?
- Kakav utjecaj ima periodičnost AF?
- Kakve AF algoritam pronalazi za dublje arhitekture?
- Kakav je utjecaj tabu liste na ostalim problemima?