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

Sadržaj

Uvod

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

Implementacijski napadi

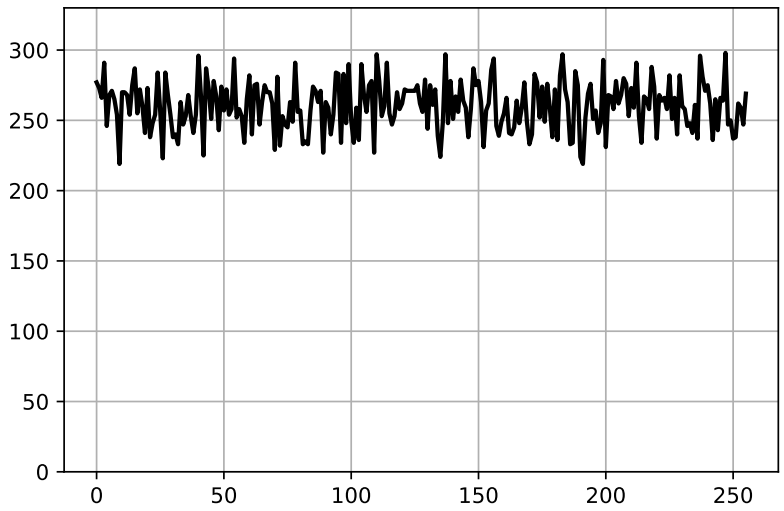
- Pretpostavka: emitirane informacije i sadržaj registara su korelirani
- Cilj: otkriti tajni ključ na temelju izmjerenih emisija (razlučitelj)
- Uvjeti: uređaj mora biti uključen i mora sadržavati tajni ključ
- Postoji više vrsta napada, grupirani su u aktivne i pasivne

Analiza potrošnje električne energije

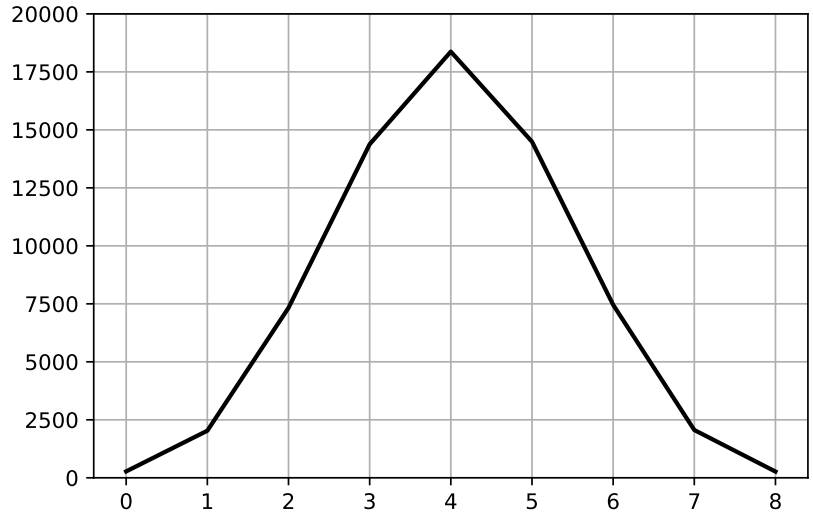
- Ideja: iskoristiti korelaciju između potrošnje el. energije uređaja i podataka zapisanih na uređaju
- Napad koji je iznimno teško detektirati
- Postoji više pristupa, među najpoznatijim je diferencijalna analiza potrošnje el. energije

Podatkovni skupovi

- Napad na AES-128
- Ulaz: trag potrošnje el. energije, reduciran Pearsonovom korelacijom
- Izlaz: predikcija vrijednosti okteta ili Hammingove težine
- DPAv2: FPGA implementacija
- DPAv4: programska implementacija



(a) Vrijednosti okteta, DPAv4



(b) Hammongove težine, DPAv4

Odabir arhitekture

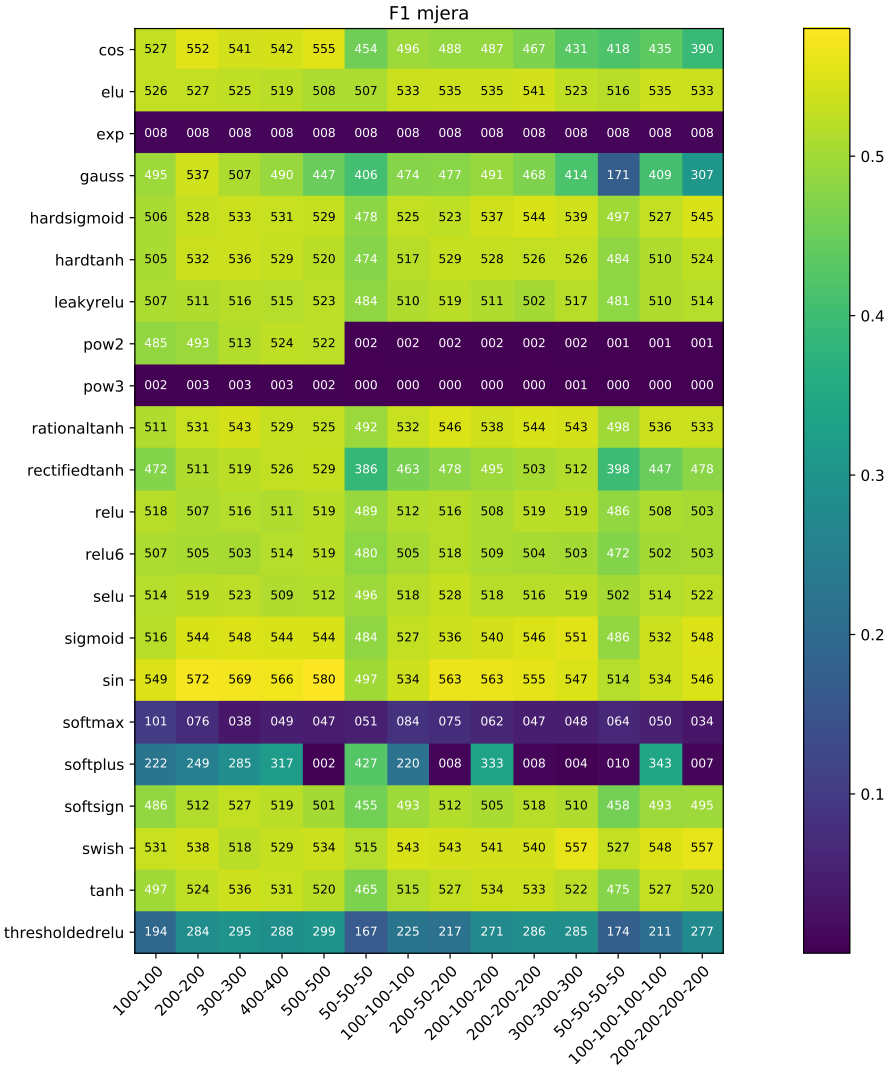
Neuronska mreža

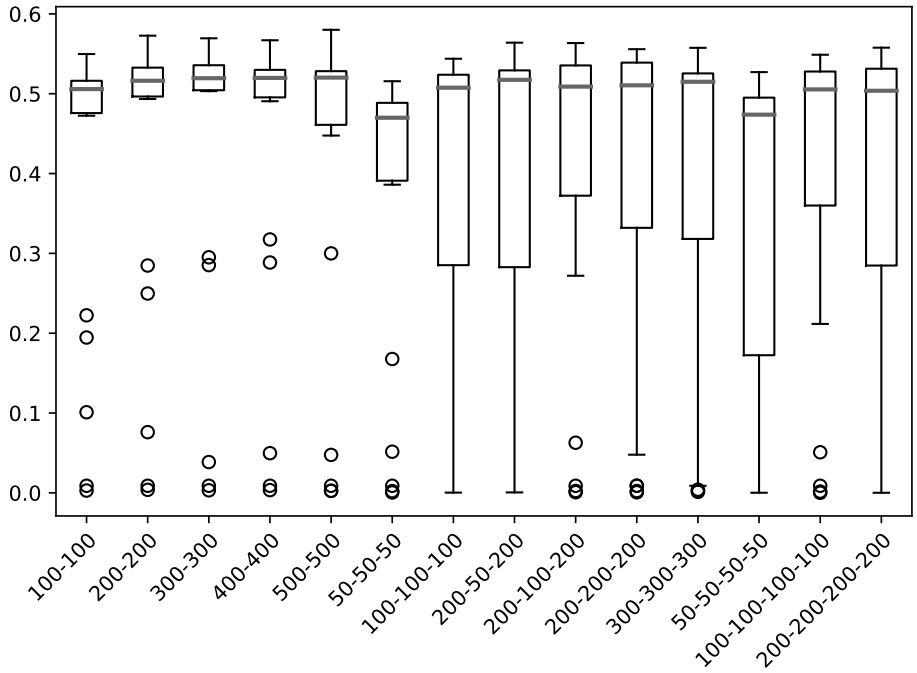
- Arhitektura: potpuno povezana, relativno plitka (do 4 skrivena sloja)
- Optimizacija: Adam, smanjivanje stope učenja, rano zaustavljanje
- Regularizacija: L2, normalizacija grupom

Pretraga hiperparametara po rešetki

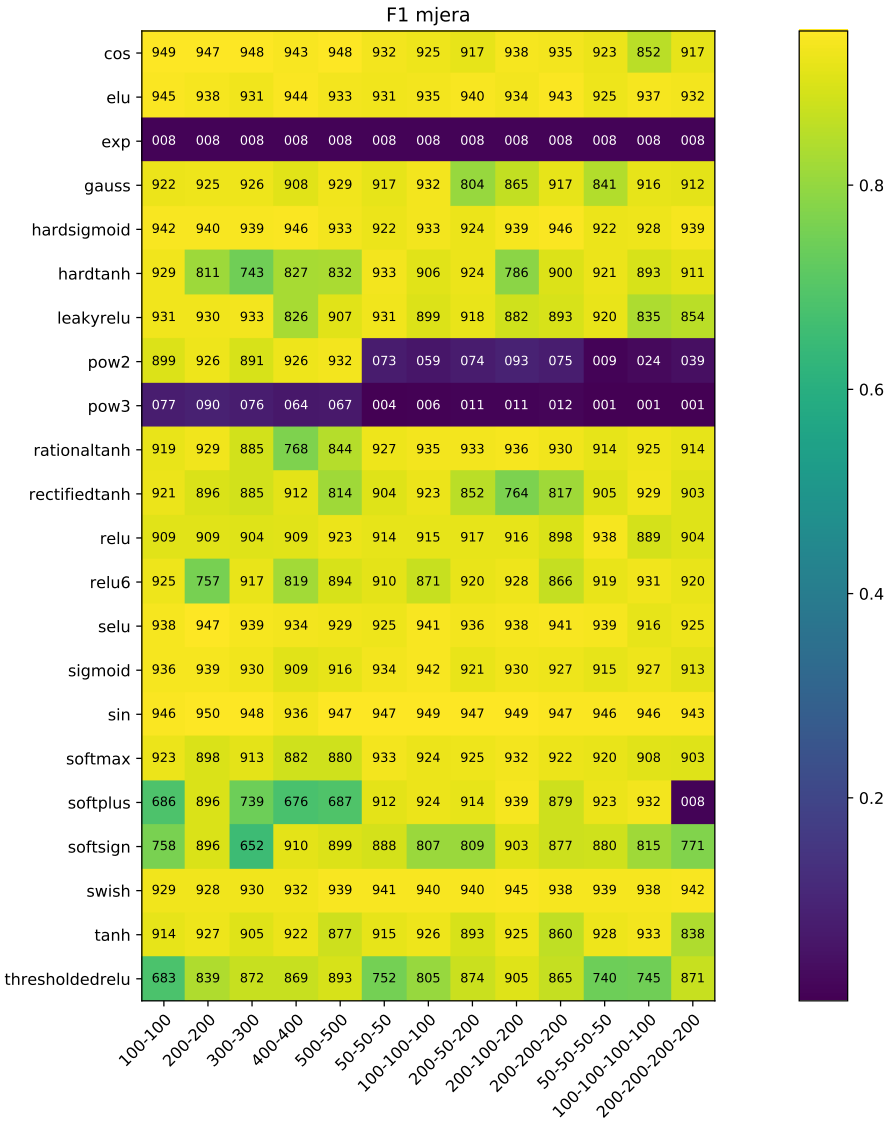
- Optimizacija stope učenja i L2 koeficijenta
- Usporedba arhitektura i aktivacijskih funkcija
- Odabir arhitektura, optimalnih za većinu funkcija
- F1 mjera – harmonijska sredina preciznosti i odziva (makro)

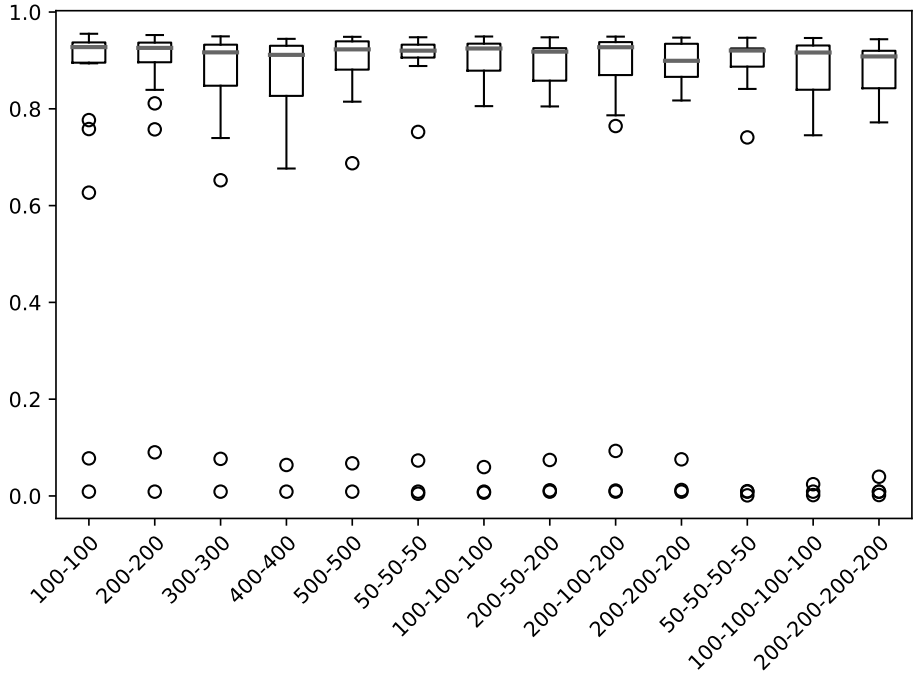
Rezultati DPAv4 (oktet)





Rezultati DPAv4 (HW)





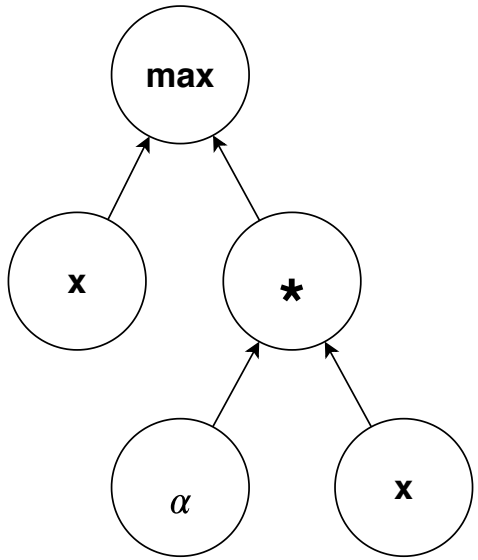
Izgradnja aktivacijskih funkcija

Genetsko programiranje

- Populacijski algoritam
- Tabu lista
- Paralelna evaluacija

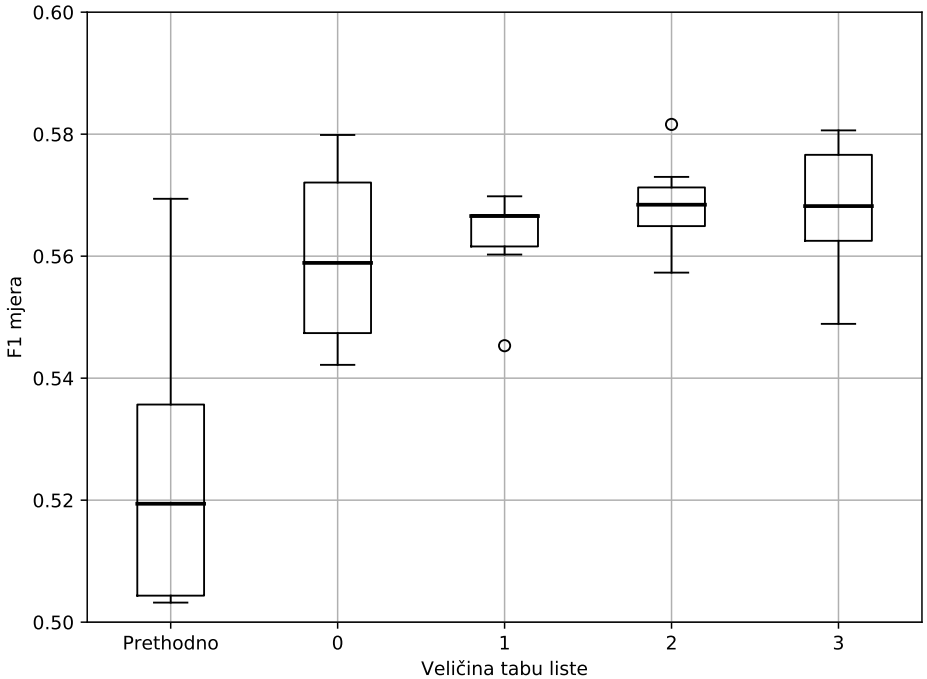
Evolucija aktivacijske funkcije

- AF kao simboličko stablo
- Čvorovi:
  ulaz, konstanta, matematičke op. i popularne AF
- Po nekoliko operatora križanja i mutacije
- Usporedba rezultata po veličini
  tabu liste s prethodno ostvarenim (rešetkom)

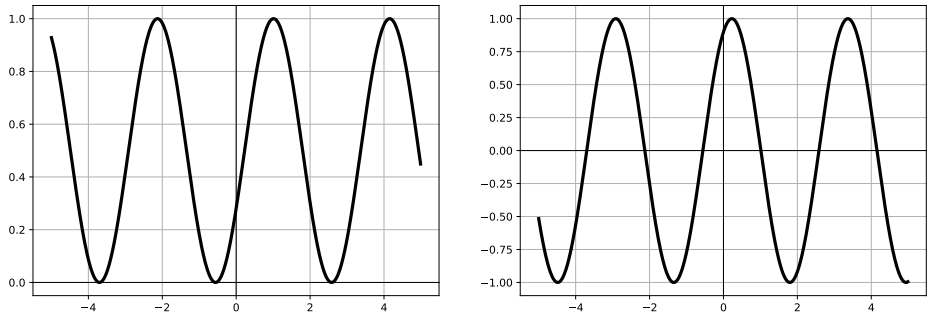


Slika: Funkcija LReLU

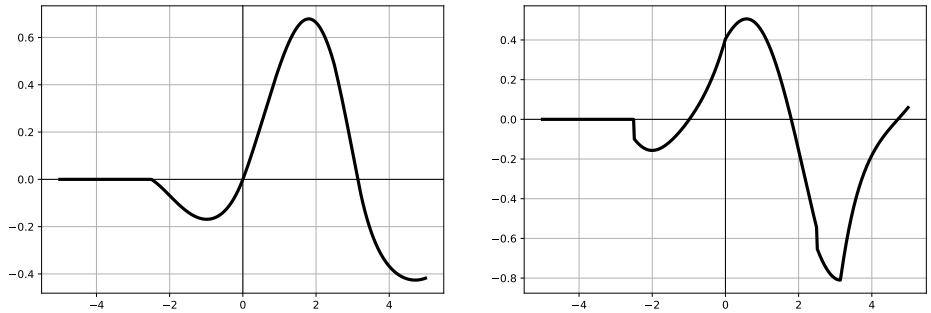
Rezultati DPAv4 (oktet)



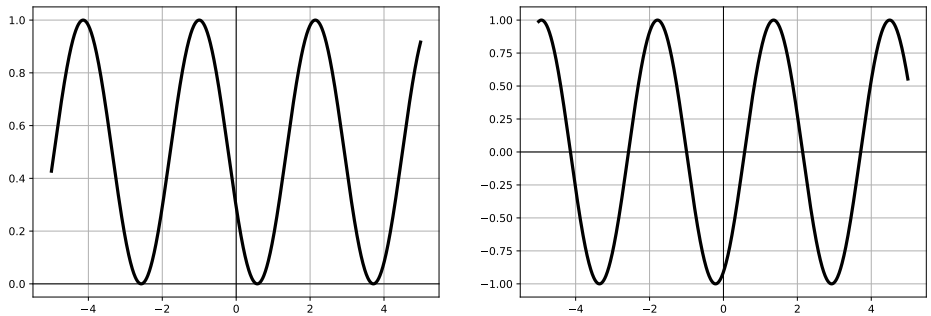
$(\cos(x - 4.153574932708071))^2$



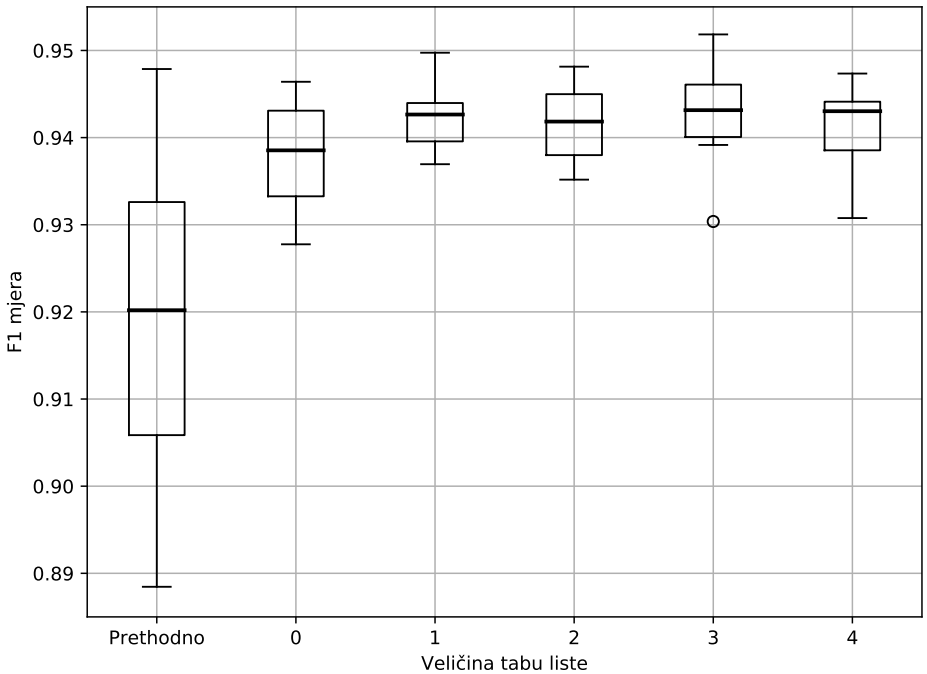
$elu(elu(\min(1.0, \min(1.0, hsigm(x)) \cdot 0.8102254104210314) \cdot \sin(x)))$



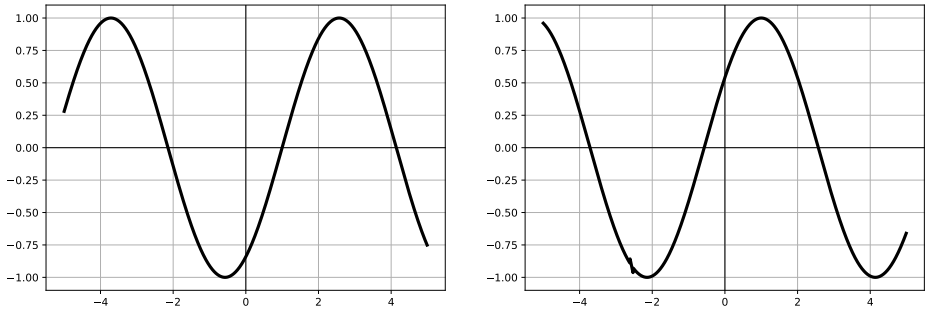
$(\cos(1.0 + x))^2$



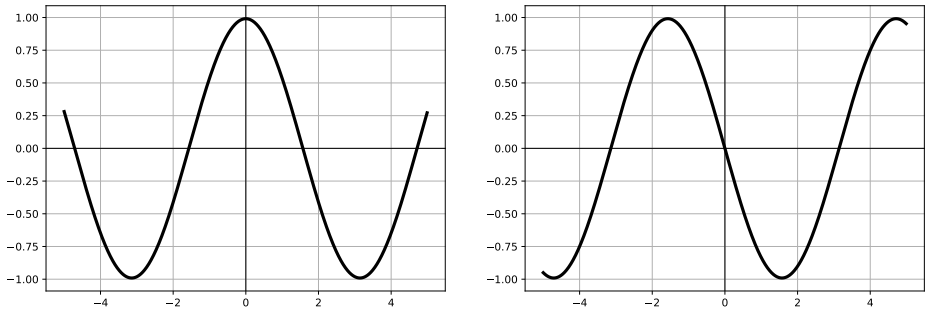
Rezultati DPAv4 (HW)



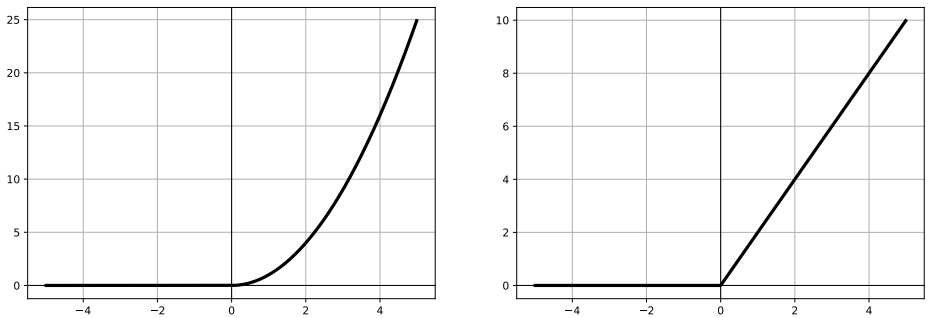
$\sin(\min(\sin(\min(x, 0.5068783911631836) + 1.0), -0.9990098031722499) + x)$



$\cos(x) \cdot 0.9910098031767487$



$ReLU(abs(x) \cdot x)$



Zaključak

- 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 širem skupu evolucijskih algoritmima i problema na kojima se primijenjuju?