ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი

# ნეირონული ქსელების გამოყენება კრიპტოგრაფიულად მედეგი ფსევდოშემთხვევითი გენერატორის ასაგებად

ჯაბა გედენიძე
ხელმძღვანელი: ზურაბ ქოჩლაძე

- ნაკადური შიფრები
- ნაკადური შიფრების გამოყენება
- ნაკადური შიფრებისთვის გამის გამომუშავება
- ფსევდოშემთხვევითი რიცხვების გენერატორები
- მრავალშრიანი ნეირონული ქსელი
- ნეირონულ ქსელზე დაფუძნებული ფსევდოშემთხვევითი რიცხვების გენერატორი

# ნაკადური შიფრები

- წარმოადგენენ სიმეტრიული შიფრებს;
- გასაღებების ნაკადის (**გამის**) გამომუშავება ხდება გასაღებისა და სპეციალური ალგორითმით;
- ნაკადური შიფრები აპარატურული შესრულებით სწრაფია;

## ნაკადური შიფრების ტიპები:

- სინქრონული ნაკადური შიფრები;
- თვითსინქრონიზებადი ანუ ასინქრონული ნაკადური შიფრები;
- ბინარულ ადიტიური ნაკადური შიფრი;

# სინქრონული ნაკადური შიფრები

- გამის გამომუშავება ხდება ღია ან შიფროტექსტისგან დამოუკიდებლად. დაშიფვრის პროცესი შეიძლება აღიწეროს შემდეგნაირად:

$$\sigma_{i+1} = f(\sigma_i, k)$$

$$z_i = g(\sigma_i, k)$$

$$c_i = h(z_i, m_i)$$

# ასინქრონული ნაკადური შიფრები

- გამის გენერირებაში მონაწილეობს გასაღები და ასევე შიფროტექსტის მუდმივი, n რაოდენობის ბიტი. ეს პროცესი შეიძლება აღვწეროთ შემდეგი სახით:

$$\sigma_i = (c_{i-n}, c_{i-n+1}, \ldots, c_{i-1})$$

$$z_i = g(\sigma_i, k)$$

$$c_i = h(z_i, m_i)$$

# ფსევდოშემთხვევითი მიმდევრობები

## ფსევდოშემთხვევითი ბიტების გენერატორი.

- დეტერმინირებული ალგორითმი;
- *k* სიგრძის შემთხვევით მიმდევრობიდან გამოიმუშავებს *l* სიგრძის შემთხვევით მიმდევრობას (*k* < *l* );
- მოწინააღმდეგემ ვერ უნდა გაარჩიოს მიღებული მიმდევრობა შემთხვევითია თუ არა;

# ძვრის წრფივი უკუკავშირიანი რეგისტრი (LFSR)

- L სიგრძის ძვრის წრფივი უკუკავშირის რეგისტრი შეიცავს L რეგისტრს (0,1,2,…,L-1) თითოეულ მათგანს შეუძლია ერთი ბიტის მიღება, შენახვა და გადაცემა.

- LFSR სტრუქტურა შეიძლება აღვწეროთ $C(X) = 1 + c_1 X + c_2 X^2 + ... + c_L X^L \in Z_2[X]$ პოლინომის საშუალებით, აღინიშნება $\langle L, C(X) \rangle$ სიმბოლოთი

1. ნულოვან რეგისტრში მოთავსებული ბიტი ხდება გამოსასვლელი მიმდევრობის ერთი ბიტი;

2. i-ური რეგისტრის ბიტი გადაეცემა i-1 რეგისტრს ყველა i- თვის

$$1 \leq i \leq L-1$$

3. ახალ შესასვლელს L-1 რეგისტრისათვის წარმოადგენს უკუკავშირის ბიტი $s_i$ რომელიც გამოითვლება ფიქსირებული რეგისტრების მნიშვნელობების XOR-ით შეკრების გზით;

# წრფივი სირთულე

- $S^n$ მიმდევრობისათვის წრფივ სირთულეს გააჩნია შემდეგი თვისებები:

- $S^n$ ქვემიმდევრობის წრფივი სირთულე აკმაყოფილებს $0 \le L(s^n) \le n$ უტოლობას ნებისმიერი n>1

- $L(s^n) = 0$ მაშინ და მხოლოდ მაშინ, როდესაც $S^n$ არის n სიგრძის ნულოვანი მიმდევრობა

- $L(s^n) = n$ მაშინ და მხოლოდ მაშინ, როდესაც $s^n = 0,0,\ldots 0,1.$

- თუ s არის პერიოდული მიმდევრობა პერიოდით N, მაშინ $L(s) \le N$

- $L(s \oplus t) \le L(s) \oplus L(t)$

# ამოცანის დასმა

- ნაკადური შიფრი ფართოდ გამოიყენება კრიპტოგრაფიაში
- საიმედო გამის გამომუშავება დაკავშირებულია გარკვეულ სიძნელეებთან
- არსებობს გამის მისაღები ფსევდო შემთხვევითი რიცხვების გენერატორები
- ყველაზე კარგია ცალმხრივმიმართულ ფუნქციაზე დაფუძნებული გენერატორები, მაგალითად RSA და Blum Blum Shub.
- RSA გენერატორის ნაკლი არის ის, რომ ის არის საკმაოდ ნელი გენერატორი.
- ნეირონული ქსელის მეშვეობით აგებული გენერატორის უპირატესობები:
  - სისწრაფე
  - გამოიმუშავებს საიმედო გამას

# RSA გენერატორი

- RSA ალგორითმის მოდიფიკაცია

საწყისი პარამეტრები:

- მოდულის ფუძე n=pq,
- e რიცხვი, რომლისთვისაც

$$(e, \phi(n)) = 1$$

სადაც, $\varphi(n) = (p-1)(q-1)$

- ღია ტექსტი M
- დამშიფრავი ფუნქცია: $C = M^e \bmod n$

# ნეირონული ქსელები

- ნეირონული ქსელი წარმოადგენს ადამიანის ტვინის გამარტივებულ მოდელს
- ნეირონული ქსელების გამოყენების სფეროები:
  - კლასიფიკაციის და პროგნოზირების ამოცანები
- თითოეული ნეირონი, როგორც ქსელის ელემენტი, აღიწერება თავისი წონების ერთობლიობით, ზღრუბლების მნიშვნელობებით და f - აქტივაციის ფუნქციით.

აქტივაციის ფუნქცია ƒ - შეიძლება იყოს შემდეგი სახის:

1.ზღრუბლური ფუნქცია (threshold function),

ƒ (u)=1, თუ u ≥0

ƒ (u)=0, თუ u<1

2. სიგმოიდური ფუნქცია (Sigmoid function)

ƒ (u)=$1/(1+e^{-bu})$ , სადაც b>0

3. უბან-უბან წრფივი ფუნქცია (pice -wise -function)

ƒ (u)=1,თუ u>0,5

ƒ (u)=|u|,თუ |u|<0,5

ƒ (u)=0, თუu<0,5

4. ფუნქცია ნიშანი (signum)

ƒ (u)= -1, თუ u <0

ƒ (u)= 1, თუ u ≥0

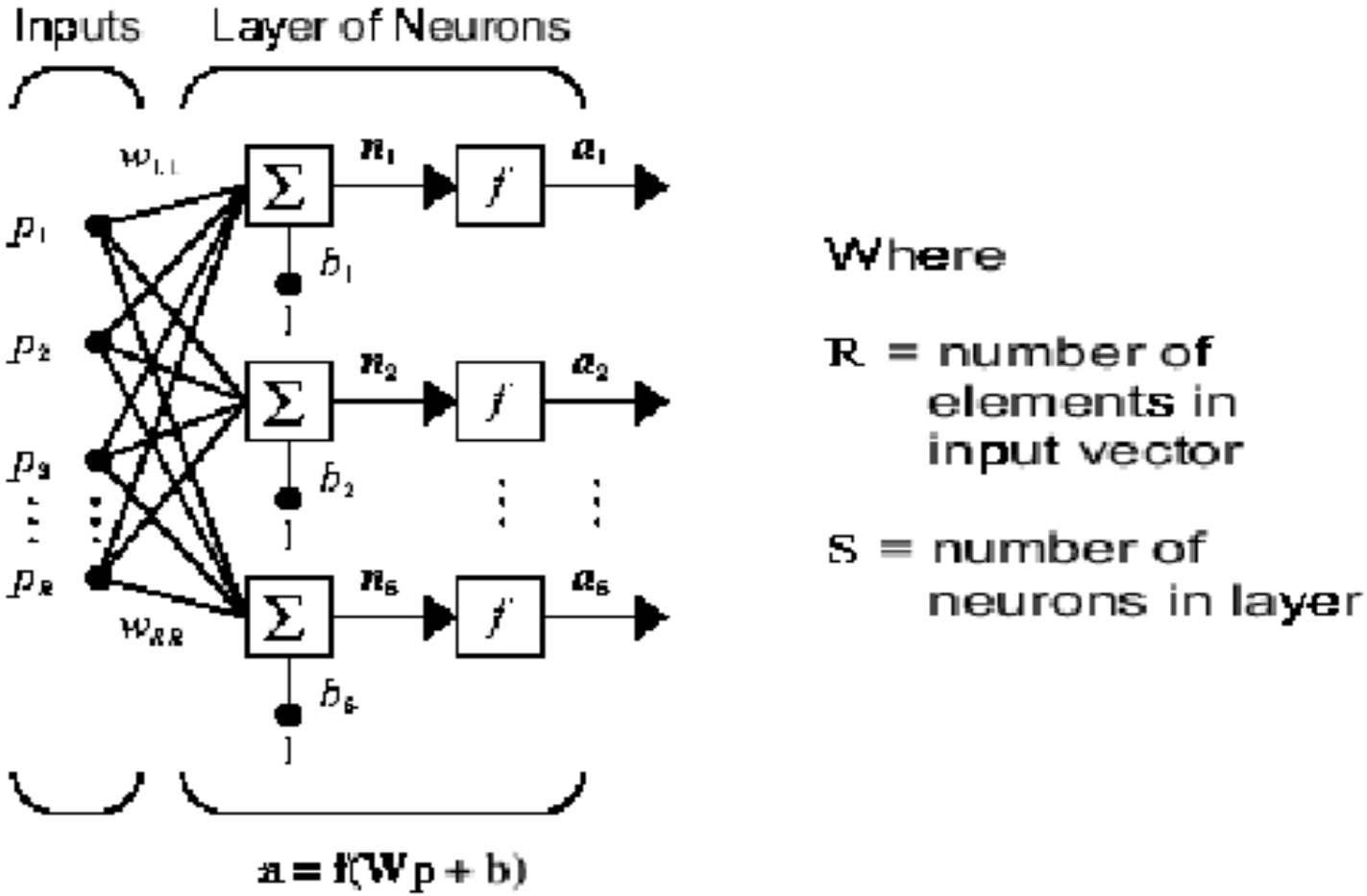
# ქსელის სწავლება

- სწავლება მასწავლებლით
- სწავლება მასწავლებლის გარეშე

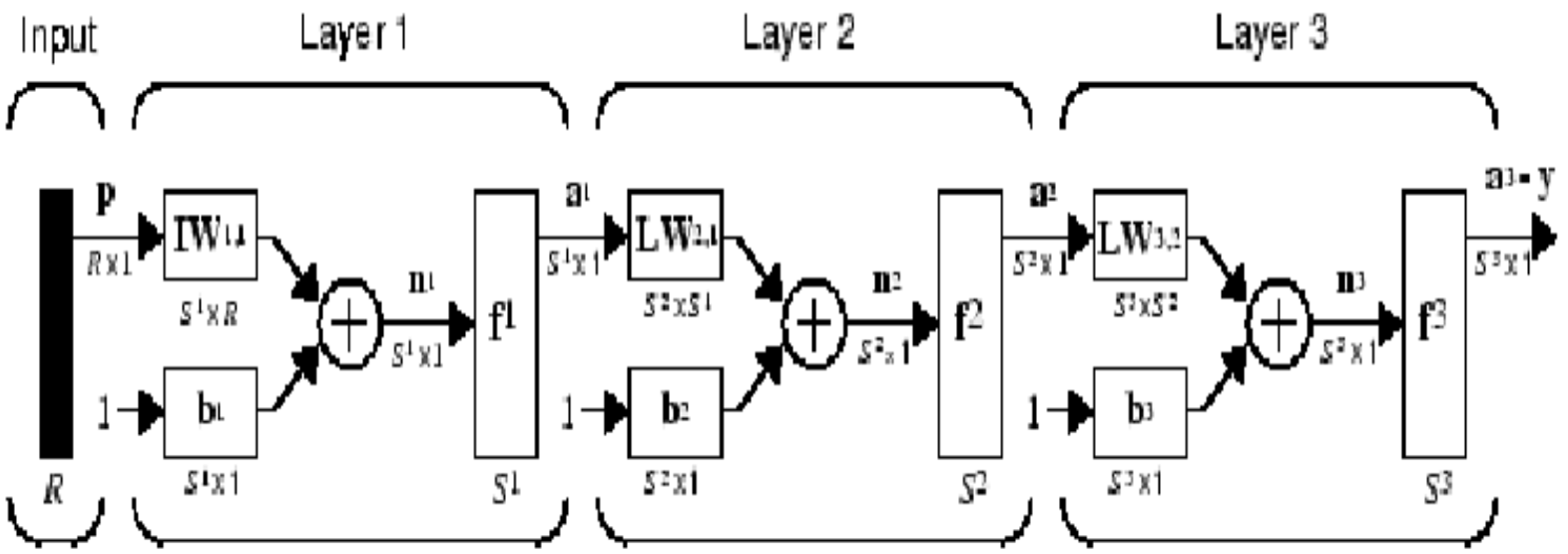
# მრავალშრიანი ნეირონული ქსელი (MLP)

მრავალშრიანი პერცეპტრონი შედგება სამი ან მეტი შრისგან:

- შემავალი შრე
- ერთი ან მეტი ფარული შრე
- გამომავალი შრე




სურათი 1. ერთშრიანი ნეირონული ქსელის მოდელი




სურათი 2. მრავალშრიანი ნეირონული ქსელის მოდელი

# მრავალშრიანი ნეირონული ქსელი (MLP) როგორც ფსევდო შემთხვევითი რიცხვების გენერატორი.

- MLP-ზე დაფუძნებული შემთხვევითი რიცხვების გენერატორები წარმოადგენენ მძლავრ შესაძლებლობას შემთხვევითი რიცხვების გენერირებისთვის.

# დელტა წესი

- იყენებს ტიპიურ სიგმოიდური (ლოგისტიკური) აქტივაციის ფუნქციას :

$$f(NET) = 1/(1+e^{-\lambda net})$$

- სადაც, $NET = \sum w_i x_i$

- λ - ამოზნექილობის პარამეტრი, განსაზღვრავს გადასვლის სიმრუდეს.

- დელტა-წესი ქსელის წონითი კოეფიციენტის რეგულირებისათვის:

$$\Delta w_k = c(d_i - O_i) f'(net_i) x_i$$

- $c$ სწავლების სიჩქარის მუდმივი კოეფიციენტი,
- $d_i$ და $O$ ნეირონის მოსალოდნელი და რეალური გამოსასვლელები,
- $f'$ i- ური კვანძის აქტივაციის ფუნქციის წარმოებული
- $x_j$ i- ური კვანძის j-ური შესასვლელის მნიშვნელობა.

# შეცდომის უკუგავრცელების მეთოდი

- დელტა-წესის განზოგადოება

- ქსელების სწავლების პრობლემის გადაწყვეტის საშუალება

- წონითი კოეფიციენტის ცვლილება შესასვლელი შრის კვანძებისათვის გამოითვლება ფორმულით:

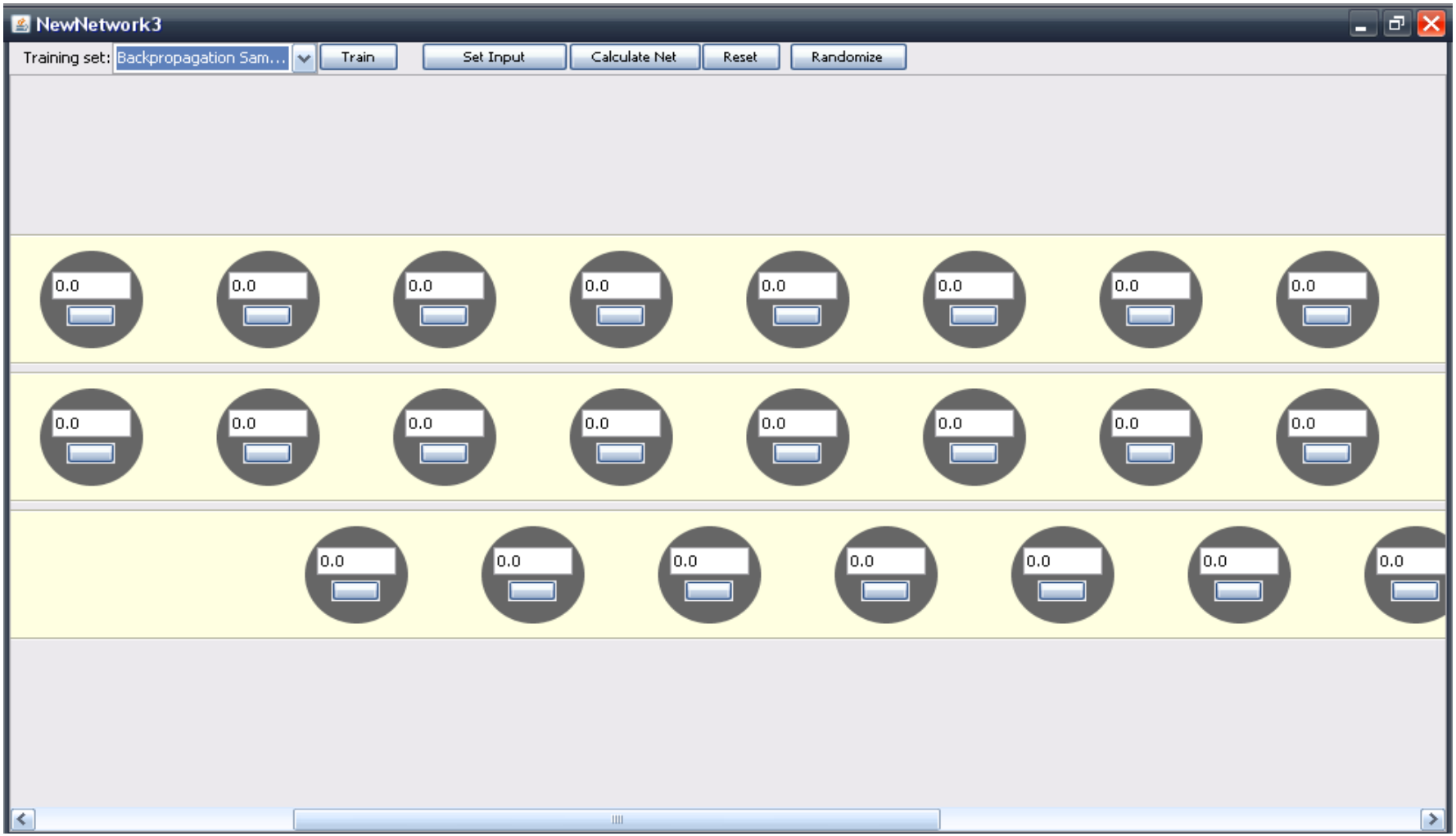
$$\Delta w_{ki} = -\lambda c(d_i - O_i)O_i(1-O_i)x_k$$

- დაფარული შრეების კვანძებისათვის:

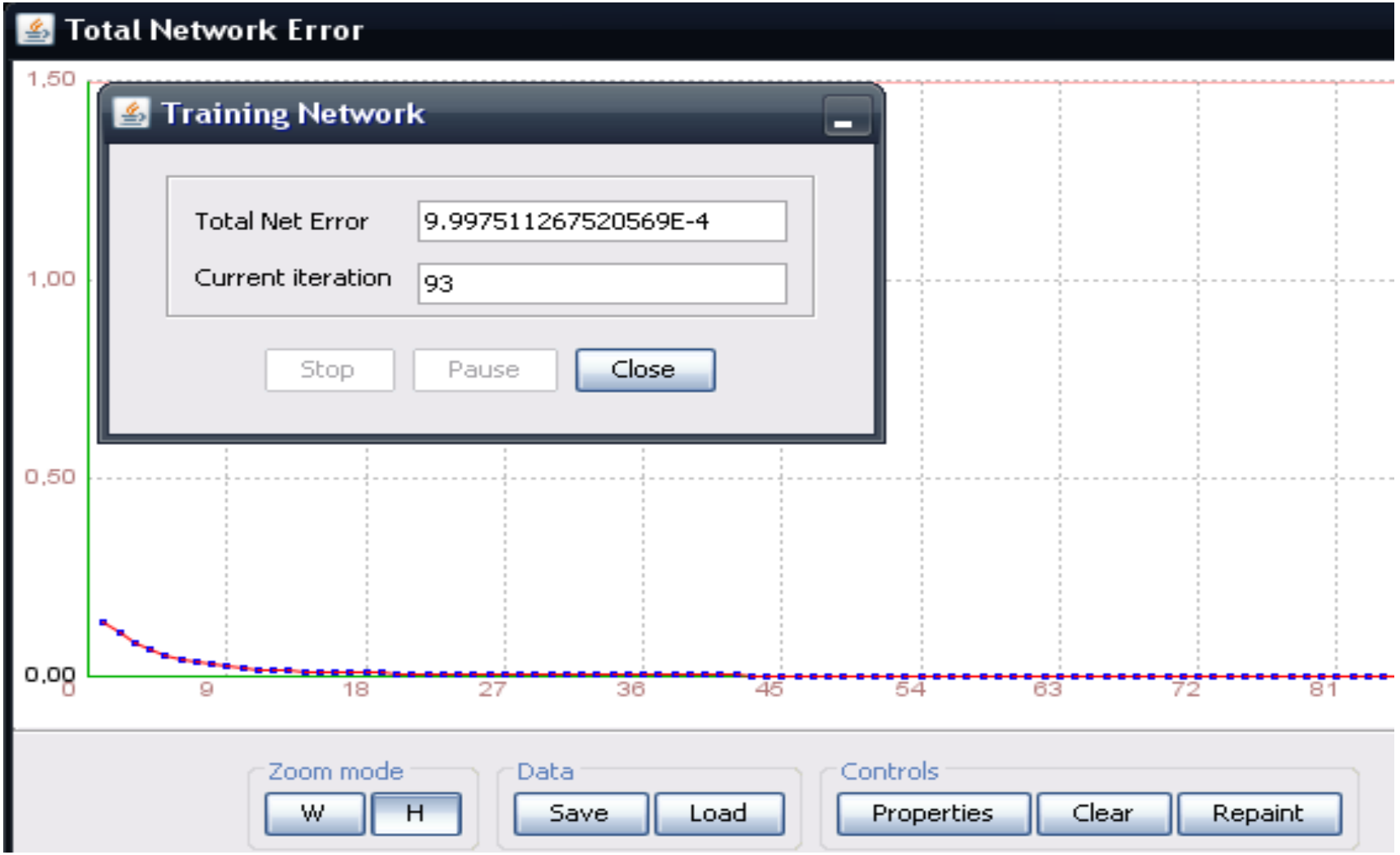
$$\Delta w_{ki} = -\lambda c O_i(1-O_i)\sum_j(-delta_j w_{ij})x_k$$

$$delta_j = -\frac{\partial E}{\partial net_j} = (d_i - O_i)O_i(1-O_i)$$

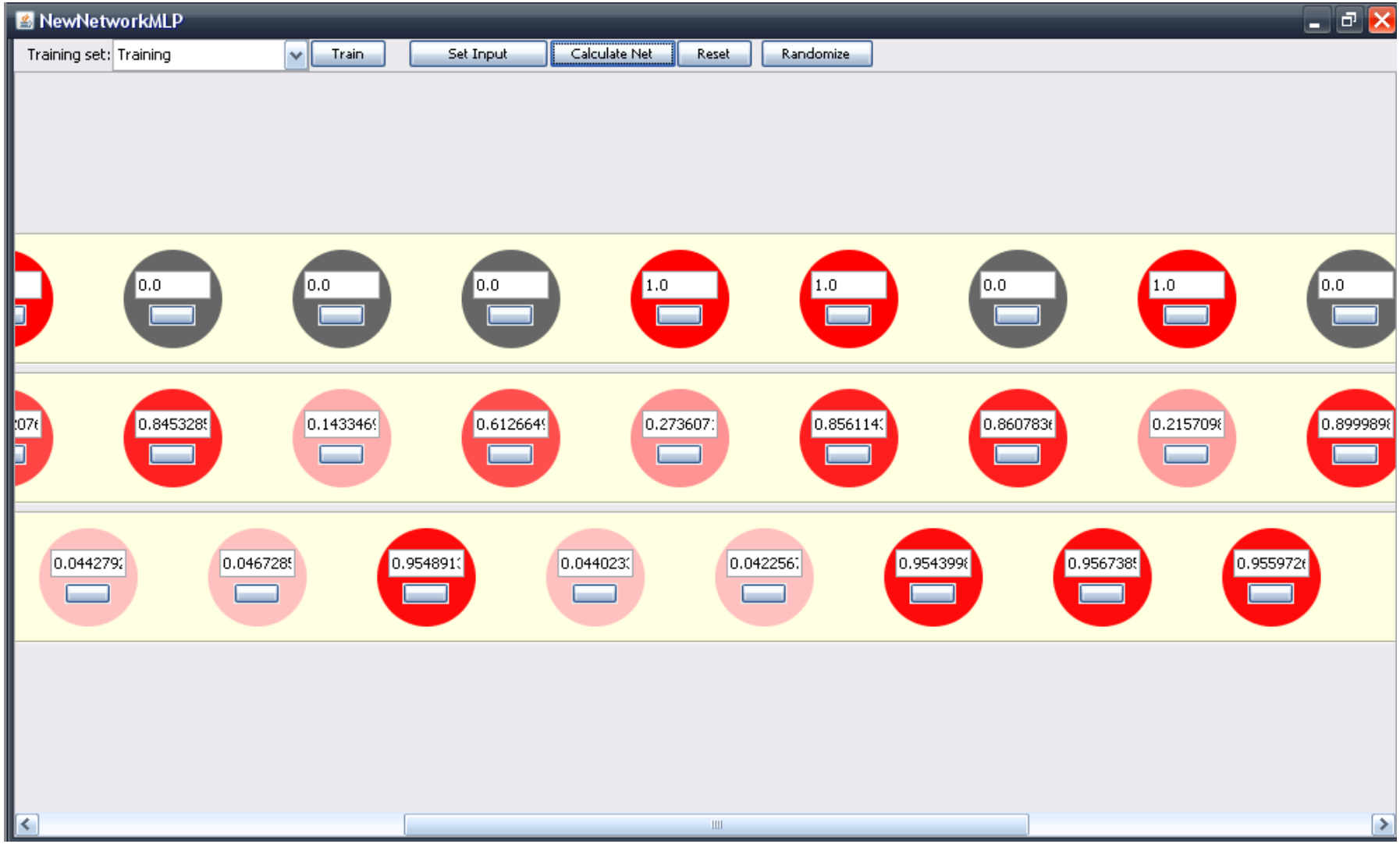
# ნეირონული ქსელით ფსევდოშემთხვევითი მომდევრობების გამომუშავება




MLP ნეირონული ქსელი




ნეირონული ქსელის სწავლების პროცესი




მრავალშრიანი ნეირონული ქსელი შემავალი და გამომავალი მიშვნელობებით

- ცდებმა აჩვენა, რომ ნეირონული ქსელი გვაძლევს კარგ მიმდევრობას ნაკადურ შიფრებში გამოსაყენებლად.

- ნეირონული ქსელის სწავლებაზე და ქსელით მიმდევრობების მიღებაზე იხარჯება ნაკლები დრო ვიდრე RSA გენერატორით მიმდევრობების გამომუშავებაზე.