Neural PRNG

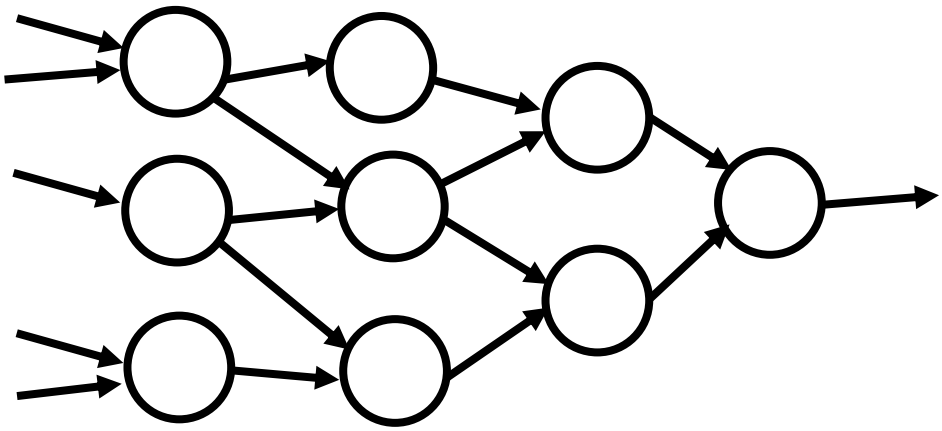
Entwicklung von JAVA-Anwendungen auf Android Studio

Kohärente PRNGs in neuronalen Netzen

*Kohärent – mehrere PRNG-Instanzen erzeugen unabhängig voneinander identische Arrays von Pseudozufallszahlen mit denselben Startwerten (mit demselben Hauptschlüssel).

** Der Hauptschlüssel hat hier die Bedeutung der Startbedingungen.

Darüber hinaus verfügen solche Generatoren nicht über einen konstanten Generierungsalgorithmus (er kann sich in jedem Schritt ändern) und können grundsätzlich nie wiederholt werden (Wiederholungen können vermieden werden).



Die Auswahl an möglichen Optionen ist riesig.

Zum Beispiel. Ein Teil des Hauptschlüssels wird verwendet, um die Anzahl der Neuronen und Schichten zu berechnen und Neuronen auf die Schichten zu verteilen. Der andere Teil des Hauptschlüssels bestimmt die Anzahl der Verbindungen und deren Verteilung auf die Neuronen. Der dritte Teil des Hauptschlüssels gibt die Gewichtungen und Offsets an.

Für einen bestimmten Datensatz werden mehrere (Zehner, Hunderte, Tausende ...) Trainingszyklen durchgeführt.

Danach kann ein solches „neuronales Modul“ in einem PRNG verwendet werden.

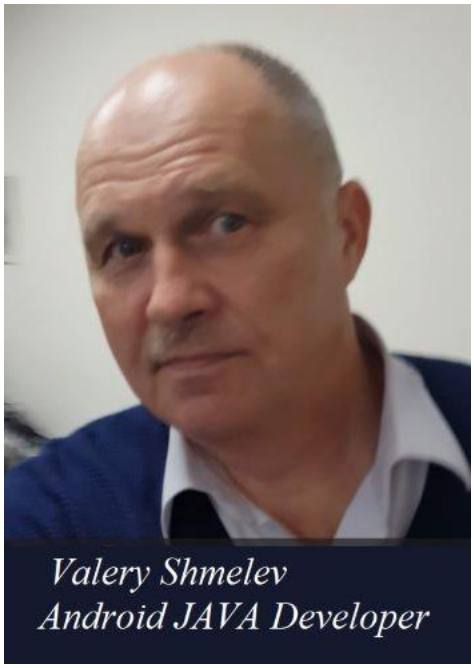
Das einfachste Beispiel. Die Ausgabewerte jedes Neurons (Big Int) werden verwendet, um das nächste Primzahlenpaar für den Bloom-Blum-Shub-Algorithmus zu finden.

Aus dem erhaltenen Ergebnis wird das Paritätsbit verwendet. Dann wird der nächste Arbeitszyklus durchgeführt. Die Eingabe sind die berechneten ungenutzten Daten. Es stellt sich noch ein bisschen heraus. Und so weiter, bis der Big Int eine „zufällige“ Zahl der erforderlichen Dimension generiert.

Und das ohne zusätzliches Training des Generators und ohne Neukonfiguration des neuronalen Netzwerks.

Ein solches PRNG wird nicht schnell sein. Aber solche Pseudozufallszahlengeneratoren sind im Hinblick auf die Bekämpfung der Kryptoanalyse sehr interessant.

Versuchen wir als Nächstes, das einfachste „neuronale“ PRNG zu erstellen.



PS. Diese Projekte sind eine hervorragende Grundlage für Ihre eigenen Entwicklungen.

Eines der „dynamischen“ Projekte (eine konsistente Reihe von JAVA-Projekten in der Entwicklung) ist das neuronale Netzwerk SimpleNNeuron auf Android JAVA. Tatsächlich, wie man ein einfaches neuronales Netzwerk schreibt und trainiert.

http://multidoc.oflameron.com/page004.htm

http://site.oflameron.ru/page005.htm

http://webpage.pips.ru/page0006.htm