Mathematik / Informatik

Thema: **Schnelle, echte Zufallszahlen? Zufallszahlen auf Diodenbasis!**

Teilnehmer	Anschrift	Schule / Institution / Betrieb
Sebastian Kollmeyer (16)	Ober-Ramstadt	Edith-Stein-Schule Darmstadt
Betreuer/in	Franz Bönsel	Projekt Nr. 150301

Um Session Keys für das gängige hybride Verschlüsselungsverfahren zu erhalten, benötigt man zufällige Binärzahlen. Damit das hybride Verschlüsselungsverfahren auch sicher ist, müssen diese Zahlen rein zufällig sein. Zufallszahlen aus Computerprogrammen sind allerdings nur Pseudozufallszahlen, da diese auf Basis eines Algorithmus erzeugt wurden.

In der Theorie ist die beste Variante, um echte Zufallszahlen zu erhalten, Zufallsgeneratoren auf Basis physikalischer Effekte zu nutzen. Ein Beispiel hierfür ist der Avalanche Effekt, der an einer Z-Diode auftritt. Doch wie zufällig sind diese Zahlen in der Praxis? Das wird in diesem Projekt untersucht.

Auf Basis einer Z-Diode wurde ein Rauschgenerator gebaut, aus dem mit einem Analog Digital Umsetzer die zu untersuchenden Zahlen gewonnen werden. Dazu wurde mit einem FPGA Board und der Hardwarebeschreibungssprache VHDL ein Mikrochip entwickelt, um aus dem Rauschen möglichst effektiv Zufallszahlen zu generieren und anschließend an einen Computer zu schicken. Um zu überprüfen, ob es sich bei den gewonnenen Zahlen tatsächlich um Zufallszahlen handelt, werden diese verschiedenen statistischen Tests unterzogen.

Das Ergebnis: Es ist tatsächlich anzunehmen, dass die generierten Zahlen zufällig sind. Somit lassen sich mit diesem Verfahren schnell und einfach echte Zufallszahlen generieren.

Stand: 02.02.2018 20:03 Uhr