

Mathematik/Informatik

Thema: Zufallszahlen auf Diodenbasis

| | | |
|--------------------------|---------------|--------------------------------|
| Teilnehmer | Ort | Schule / Institution / Betrieb |
| Sebastian Kollmeyer (17) | Ober-Ramstadt | Edith-Stein-Schule, Darmstadt |
| Betreuer/in | Franz Bönsel | Projekt Nr. 73032 |

Zur sicheren Verschlüsselung benötigt man zufällige Binärzahlen. Damit ein 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 USB Stick entwickelt, der eine hohe Zahl an Zufallszahlen erzeugt und diese an einen Computer sendet. Diese können anschließend mit einem Programm abgerufen werden. Die Zahlen wurden anschließend verschiedenen statistischen Tests unterzogen. Dabei konnte festgestellt werden, dass sich die Zahlen tatsächlich zufällig verhalten.

Stand: 12. Februar 2019, 18:25 Uhr