

Sparte

Jugend forscht

Fachgebiet

Mathematik/Informatik

Thema

Nichtlineare Permutationen für kryptographische Anwendungen

Teilnehmer / Name

Schule / Institution / Betrieb

Sebastian Riemann

Universität Rostock, Institut für Mathematik

Betreuung

Prof. Dr. Gohar Kyureghyan

Universität Rostock, Institut für Mathematik

Björn Kriepke

Universität Rostock, Institut für Mathematik

In diesem Projekt habe ich mich mit nichtlinearen Permutationen für kryptographische Anwendungen beschäftigt. Solche Permutationen sind ein zentraler Bestandteil moderner Hashfunktionen und symmetrischer Verschlüsselungsverfahren.

Das Ziel des Projektes ist es, solche Permutationen algorithmisch und theoretisch zu studieren. Dazu habe ich eine bereits bekannte Permutation genauer untersucht und eine wichtige kryptographische Eigenschaft dieser bewiesen. Zusätzlich habe ich mittels theoretischer Überlegungen und computergestützter Suche die Funktion verbessern können. Weiterhin habe ich eine neue Methode gefunden, um Funktionen in beliebigen Dimensionen zu konstruieren.

In Zukunft plane ich diese Methode weiterzuentwickeln, um nach neuen kryptographisch stärkeren Funktionen zu suchen.