Algorithmen zur Struktur-Analyse des von A5/1 induzierten Graphen

Master Thesis von Michael Bacher

Kurzbeschreibung

In dieser Masterarbeit soll gezeigt werden, wie man die Qualität von GSM Sprachverschlüsselung beurteilen kann. Dazu muss man die Struktur des Zustandsgraphen analysieren, welcher durch den Verschlüsselungsalgorithmus A5/1 erzeugt wird. Der Algorithmus A5/1 ist ein Pseudozufallszahlengenerator, welcher in der GSM-Mobilfunktechnik eingesetzt wird.

Es sollen Algorithmen entwickelt werden, mit denen man die Struktur von Zustandsgraphen analysieren kann, die durch Pseudozufallszahlengeneratoren induziert werden. Im speziellen wird der durch A5/1 induzierte Graph untersucht.

Der Verschlüsselungsalgorithmus A5/1 ist ein besonders schönes Beispiel für den Verstoß gegen das Kerckhoffsche Prinzip (security by obscurity): Die Stärke der Verschlüsselung liegt im Geheimnis des Algorithmus. Dabei stellt sich die Frage, was die Entwickler im Design des symmetrischen Verschlüsselungsalgorithmus A5/1 verstecken wollten?

Der Autor dieser Masterarbeit möchte gerne in Theorie und Praxis den technologischen Hintergrund des A5/1 beleuchten. Daher werden auf der theoretischen Seite die notwendigen Grundlagen der Mathematik, Zahlentheorie, Theoretischen Informatik vermittelt und die historische Entwicklung von Pseudozufallszahlengeneratoren aufgezeigt. Auf der praktischen Seite wird das Prinzip des experimentellen Prototyping angewandt und die empirischen Werte vorgestellt. Es stellt sich die Frage, ob die Schwäche bzw. Stärke des Verschlüsselungsalgorithmus A5/1 skalierbar ist, und was die „Stellschrauben“ des A5/1 sind.

Die Schwierigkeit der Analyse großer Graphen liegt mehr in der Zeit- als in der Platzkomplexität. Der induzierte Graph des Algorithmus A5/1 hat zu viele Knoten. Die Möglichkeiten, derart große Graphen trotzdem zu analysieren sind die Graphenreduktion (Sampling), das experimentelle Prototyping und die Abschätzungsverfahren.

Mit Hilfe des experimentellen Prototyping, bei dem man z.B. den Verschlüsselungsalgorithmus A5/1 funktionsgleich, aber in kleineren Dimensionen nachbaut, hat der Autor die „Stellschrauben“ von durch Mehrheitsfunktion getaktete und gekoppelte linear rückgekoppelte Schieberegister festgestellt.