idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Pressemitteilung

Ruhr-Universität Bochum
Dr. Julia Weiler

24.09.2015
http://idw-online.de/de/news638130

Forschungsprojekte
Informationstechnik, Mathematik
überregional

Verschlüsselungstechniken verbessern: Neue Emmy Noether-Nachwuchsgruppe an der RUB

Für die Entwicklung neuartiger Verschlüsselungsverfahren richtet die Deutsche Forschungsgemeinschaft an der Fakultät für Mathematik der Ruhr-Universität Bochum eine neue Nachwuchsgruppe ein. Das Team um Juniorprofessor Dr. Sebastian Faust vom Lehrstuhl für Grundlagen der Kryptographie erhält zu diesem Zweck rund 500.000 Euro für drei Jahre aus dem Emmy Noether-Programm, mit der Option auf Verlängerung um zwei Jahre und weitere 283.000 Euro Förderung.

Black Box-Modell überprüft Sicherheit kryptografischer Verfahren

Um Daten vertraulich und unversehrt in ungesicherten Netzwerken wie dem Internet zu transportieren, braucht es moderne Verschlüsselungstechniken. Bei der Entwicklung neuer Verschlüsselungsverfahren muss deren Sicherheit verifiziert werden. Die moderne Kryptografie nutzt dazu Modelle, die es erlauben, die Sicherheit von Verschlüsselungsalgorithmen mathematisch zu beweisen. So kann man potenzielle Schwachstellen in neuartigen Verfahren frühzeitig erkennen und Gegenmaßnahmen einbauen. Das am weitesten verbreitete Sicherheitsmodell in der Kryptografie ist das sogenannte Black Box-Modell, das allerdings nur eine vereinfachte Sicht auf die Realität und die Möglichkeiten eines Angreifers widerspiegelt.

Lücke zwischen Theorie und Praxis schließen

Das Black Box-Modell berücksichtigt nur Angriffe, die mathematische Schwächen des Verschlüsselungsverfahrens ausnutzen. In der Praxis zielen erfolgreiche Angriffe jedoch häufig auf Schwachstellen in der Implementation ab; das heißt, auch wenn der Verschlüsselungsalgorithmus selbst sicher ist, kann die Art und Weise, wie er zum Beispiel auf einer Chipkarte eingesetzt wird, neue Angriffe ermöglichen. Hier setzt das Forschungsvorhaben von Sebastian Faust an. „Wir wollen die Lücke zwischen der theoretischen Abstraktion des Black Box-Modells und der Realität schließen“, sagt der Mathematiker. Dazu entwickelt er mit seinem Team im Projekt „Kryptographie jenseits des Black-Box Modells“ neuartige kryptografische Verfahren, die selbst dann sicher bleiben, wenn sie in der Praxis, zum Beispiel auf Chipkarten implementiert werden.

Weitere Informationen

Jun.-Prof. Dr. Sebastian Faust, Lehrstuhl für Grundlagen der Kryptographie, Fakultät für Mathematik der Ruhr-Universität Bochum, 44780 Bochum, Tel. 0234/32-23265, E-Mail: sebastian.faust@rub.de

Juniorprofessor Dr. Sebastian Faust
© RUB, Foto: Marquard