idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Pressemitteilung

Rheinische Friedrich-Wilhelms-Universität Bonn
Dr. Andreas Archut

09.05.2005
http://idw-online.de/de/news111518

Forschungsergebnisse
Mathematik, Physik / Astronomie
überregional

Weltrekord: Bonner Forscher zerlegen riesige Zahl in Primfaktoren

Forscher der Universität Bonn und des Centrum voor Wiskunde en Informatica (CWI) aus den Niederlanden haben mit Rechnerunterstützung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) einen neuen Weltrekord im Faktorisieren aufgestellt: die Zerlegung der Zahl RSA200.

Die Sicherheit bestimmter Verfahren zur elektronischen Signatur beruht auf der Schwierigkeit, sehr große Zahlen in ihre Primfaktoren zu zerlegen. Das trifft insbesondere auf den weit verbreiteten RSA-Signaturalgorithmus zu, der 1977 von Ron Rivest, Adi Shamir und Len Adleman am Massachusetts Institute of Technology (MIT) entwickelt wurde. Das BSI untersucht kontinuierlich, welche Signaturverfahren den Vorgaben des deutschen Signaturgesetzes genügen, und dafür ist also auch eine Abschätzung des Aufwandes für solche Primfaktorzerlegungen erforderlich.

Die Zahl RSA200 hat 200 Dezimalstellen und ist das Produkt zweier Primzahlen. Sie wurde von der amerikanischen Firma RSA Security unter Geheimhaltung der Faktoren veröffentlicht, die Herausforderung bestand darin, diese beiden Zahlen zu finden.

Am jetzt aufgestellten Weltrekord waren Professor Dr. Jens Franke, Dr. Thorsten Kleinjung und Friedrich Bahr von der Universität Bonn, Peter Montgomery und Herman te Riele vom CWI aus Amsterdam sowie das BSI beteiligt.

Weitere Informationen zu Kryptoalgorithmen gibt es unter:
http://www.bsi.bund.de/esig/basics/techbas/krypto/index.htm

Die Faktoren von RSA200 finden Sie unter: http://www.loria.fr/~zimmerma/records/factor.html

Ansprechpartner für die Medien:
Professor Dr. Jens Franke
Institut für Mathematik der Universität Bonn
Telefon: 0228/73-2952
E-Mail: franke@math.uni-bonn.de
oder Dr. Thorsten Kleinjung
Telefon: 0228/73-2842
E-Mail: thor@math.uni-bonn.de

URL zur Pressemitteilung: http://www.bsi.bund.de/esig/basics/techbas/krypto/index.htm
URL zur Pressemitteilung: http://www.loria.fr/~zimmerma/records/factor.html