Institut für Algebra der TU Dresden ist neuer Weltmeister im Code knacken

Institut für Algebra der TU Dresden ist neuer Weltmeister im Code knacken
Im Institut für Algebra der TU Dresden ist in dieser Woche ein neuer Weltrekord in der Kryptographie aufgestellt worden. Der Marie-Curie-Stipendiat Dr. Jens Zumbrägel führte eine Attacke auf das sogenannte diskrete Logarithmusproblem durch, das die Grundlage für viele wichtige Arten moderner Verschlüsselungsverfahren ist, die beispielsweise beim E-Banking eingesetzt werden. Zumbrägel berechnete mit einem internationalen Forscherteam unter Verwendung eines Hochleistungsclusters einen diskreten Logarithmus in einem endlichen Körper der Größe 2 hoch 9234 (29234).
Hierdurch verbesserte das Team den alten Rekord von 2 hoch 6168 (von 26168) deutlich, was für beträchtliches Aufsehen in der Fachwelt sorgte. Darüber hinaus deckte das Team erhebliche Schwächen bei den Sicherheitsstandards für paarungsbasierte Codes mit einer bisher vermuteten Sicherheit von 2 hoch 128 (2128) Operationen auf. Dies stellt einen erfolgreichen Angriff auf einen wichtigen Typus von aktuellen Verschlüsselungsverfahren dar.
Professor Stefan E. Schmidt, Inhaber der Professur für Methoden der angewandten Algebra, ist stolz, einen so herausragenden Nachwuchswissenschaftler samt dem renommierten Marie-Curie-Stipendium für seine Arbeitsgruppe Methoden der angewandten Algebra der TU Dresden gewonnen zu haben: "Diese Attacken sind von großer Bedeutung für unsere heutigen Sicherheitssysteme, da sie einen Angriff ins Herzstück moderner Verschlüsselungstechniken, insbesondere den aktuellen identitätsbasierten Kryptosystemen, darstellen. Dies unterstreicht die zentrale Rolle einer Grundlagenwissenschaft wie die moderne Algebra für das Hinterfragen der Sicherheitsstandards unserer heutigen Informationsgesellschaft."
Die Kryptographie umfasst Themen der Konzeption, Definition und Konstruktion von Informationssystemen, die widerstandsfähig gegen unbefugtes Lesen und Verändern sind.

Informationen für Journalisten:
Prof. Dr. Stefan E. Schmidt, Professur Methoden der angewandten Algebra
Tel. 0351 463-33642, 0173-3171146
Stefan.Schmidt@tu-dresden.de
Links mit weiteren Informationen zu diesem Resultat:
 http://en.wikipedia.org/wiki/Discrete_logarithm_records
 http://ellipticnews.wordpress.com/
 https://listserv.nodak.edu/cgi-bin/wa.exe?A2=NMBRTHRY;9aa2b043.1401
<img src="http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=556646" width="1" height="1">

Pressekontakt

Technische Universität Dresden

01062 Dresden

Firmenkontakt

Technische Universität Dresden

01062 Dresden

Die TU Dresden ist eine der elf Exzellenzuniversitäten Deutschlands. Als Volluniversität mit breitem Fächerspektrum zählt sie zu den forschungsstärksten Hochschulen. Austausch und Kooperation zwischen den Wissenschaften, mit Wirtschaft und Gesellschaft sind dafür die Grundlage.Ziel ist es, im Wettbewerb der Universitäten auch in Zukunft Spitzenplätze zu belegen. Daran und am Erfolg beim Transfer von Grundlagenwissen und Forschungsergebnissen messen wir unsere Leistungen in Lehre, Studium, Forschung und Weiterbildung.Wissen schafft Brücken. Seit 1828.