Ein neuer Algorithmus stellt die Kryptographie auf den Prüfstand

Ein neuer Algorithmus stellt die Kryptographie auf den Prüfstand
Forscher des Lothringer Forschungslabors für Informatik und ihre Anwendungen (CNRS - französisches Zentrum für wissenschaftliche Forschung / Universität der Lorraine / INRIA - französisches Forschungsinstitut für Informatik und Automatik) und des IT-Labors der Universität Paris 6 (CNRS / UPMC - Universität Pierre
 Marie Curie) haben einen verbesserten Algorithmus zur Lösung einer bestimmten Variante des sogenannten diskreten Logarithmusproblems vorgestellt. Die Sicherheit zahlreicher, heute verwendeter Kryptosysteme (Datenverschlüsselungssysteme) beruht auf dem diskreten Logarithmus.
Die Forscher haben einen neuen Algorithmus entwickelt, der im Mai auf der Internationalen Konferenz Eurocrypt 2014 in Kopenhagen präsentiert wurde und auf der Website der International association of cryptologic research vorgestellt wird. Der Algorithmus ermöglicht bereits, verschiedene Verschlüsselungssysteme abzulehnen, die bisher ausreichende Sicherheit garantierten. Die Ergebnisse betreffen jedoch nur eine sehr spezielle Variante des diskreten Logarithmusproblems.
Das diskrete Logarithmusproblem wird in einer mathematischen Struktur berechnet, die man als endliche Körper bezeichnet. Die jetzt veröffentlichten Resultate betreffen aber nur sogenannte endliche Körper mit kleiner Charakteristik. Eine Bedrohung für die Sicherheit im Netz sind die Ergebnisse also im Moment nicht. Trotzdem ist nicht auszuschließen, dass in Zukunft verbesserte Angriffe die Sicherheit dieser Algorithmen in Zweifel ziehen und Auswirkungen, vor allem auf kryptographische Anwendungen von Smart Cards und RFID-Chips haben könnten. Möglicherweise gibt es eine Variation dieses neuen Algorithmus, die sich auch auf generische endliche Körper anwenden lässt.
Mit Hilfe der Kryptographie werden vertrauliche Informationen geschützt. Sie beruht auf hochmathematischen Algorithmen, die selbst mit den komplexesten Maschinen nur schwer oder gar nicht zu lösen sind.
Die Sicherheit einer der schwierigsten Varianten des diskreten Logarithmus wurde von vier Forschern des CNRS, des INRIA und vom IT-Labor der Universität Paris 6 durchbrochen. Dieser von den Forschern entwickelte Algorithmus unterscheidet sich von den besten bisher für dieses Problem bekannten Algorithmen. Zum einen ist er deutlich einfacher zu erklären und zum anderen viel komplexer: Mit ihm können immer größere Probleme des diskreten Logarithmus gelöst werden, wobei die Rechenzeit deutlich moderater ansteigt als bei bisherigen Algorithmen. Die Berechnung von diskreten Logarithmen, die absichtlich mit komplexen Problemen verbunden sind, wird stark erleichtert.
Diese Forschungsarbeiten befinden sich jedoch noch in der theoretischen Phase und der Algorithmus muss zunächst noch verfeinert werden, bevor eine praktische Demonstration der Schwäche dieser Variante des diskreten Logarithmus erfolgen kann. Dennoch zeigen diese Ergebnisse eine Lücke in der kryptographischen Sicherheit und ebnen den Weg für weitere Forschungen. Der Algorithmus könnte zudem so angepasst werden, dass sich mit ihm die Sicherheit anderer kryptographischer Lösungen testen lässt.
Quelle: "Un nouvel algorithme secoue la cryptographie", Artikel aus Techno-Science.net - 12.05.2014 - news=12781'>http: //www.techno-science.net/?onglet=news
news=12781
Redakteur: Aurélien Filiali, aurelien.filiali@diplomatie.gouv.fr

Wissenschaftliche Abteilung, Französische Botschaft in der Bundesrepublik Deutschland
Pariser Platz 5
10117 Berlin
Telefon: 030 590 03 92 50
Telefax: 030 590 03 92 65
Mail: sciencetech@botschaft-frankreich.de
URL: http://www.wissenschaft-frankreich.de
<img src="http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=566732" width="1" height="1">

Pressekontakt

Wissenschaftliche Abteilung, Französische Botschaft in der Bundesrepublik Deutschland

10117 Berlin

wissenschaft-frankreich.de
sciencetech@botschaft-frankreich.de

Firmenkontakt

Wissenschaftliche Abteilung, Französische Botschaft in der Bundesrepublik Deutschland

10117 Berlin

wissenschaft-frankreich.de
sciencetech@botschaft-frankreich.de

Die großen Herausforderungen unseres Jahrhunderts ? Umwelt, Ressourcen, Gesundheit, Ernährung, Energie ? lassen sich nur durch technologische Fortschritte meistern. Frankreich und Deutschland spielen dabei eine besondere Rolle: Durch die Bündelung ihrer Kapazitäten könnten sie angesichts ihrer jeweiligen wissenschaftlichen Exzellenz, der bereits sehr engen Verknüpfung ihrer Netzwerke und der kritischen Masse ihrer Investitionen in die Forschung und Entwicklung (10% der weltweiten Forschungsinvestitionen) zur Speerspitze Europas werden. Die Wissenschaftsabteilungen der Botschaften Frankreichs bilden einen Vorposten der französischen Forschung im Ausland. Die Aufgabe der Abteilung für Wissenschaft und Technologie der Französischen Botschaft in Deutschland ist die Intensivierung der wissenschaftlichen und technologischen Zusammenarbeit mit unserem wichtigsten Partner. 1. Durch umfassende Information: Im Dienste französischer Forscher und Unternehmen informiert sich die Wissenschaftsabteilung der Botschaft täglich über die neuesten Innovationen und Ergebnisse der deutschen Forschung und besucht regelmäßig Laboratorien von öffentlichen Einrichtungen, Universitäten und Unternehmen. 2. Durch die Unterstützung bei der Bündelung unserer Forschungskapazitäten über die Organisation von Fachseminaren und Expertenbesuchen für Forscher. Die Abteilung bildet eine Schnittstelle zwischen den deutschen und französischen Behörden mit dem Ziel einer integrierten Forschungspolitik im Dienste Europas. 3. Durch die Vermittlung der Exzellenz der französischen Forschung: Als Botschafter der französischen Forschung in Deutschland, gehört es ebenso zu den Aufgaben der Wissenschaftsabteilung, die Zivilgesellschaft, Schüler und Studenten über die wissenschaftliche Exzellenz Frankreichs zu informieren und somit dazu beizutragen, eine neue Generation von Forschern mit doppeltem kulturellen Hintergrund zu formen, die geeignet ist, im Rahmen des Europäischen Forschungsraumes die deutsch-französische Spitzenforschung nachhaltig zu gestalten. Wer sind wir? Die Abteilung für Wissenschaft und Technologie der Französischen Botschaft in Deutschland wird seit dem 1. September 2009 vom Botschaftsrat Mathieu J. Weiss geleitet.Die vorausschauende und strategische Erfassung der wissenschaftlichen Aktualität steht unter der Leitung des Botschaftsattachés Dr. Stéphane Roy. Er ist ebenfalls verantwortlich für das Kooperationsprogramm Hubert-Curien Procope.Nicolas Cluzel koordiniert den Bereich Analysen und Einflüsse.Marie de Chalup koordiniert den Bereich Partnerschaften und Kommunikation.