idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Press release

Ruhr-Universität Bochum
Meike Drießen
03/30/2023
http://idw-online.de/en/news811823

Personnel announcements, Research projects
Information technology
transregional, national

ERC Advanced Grant: Umdenken für neue und sichere Verschlüsselungen

Mit 2,5 Millionen Euro Förderung vom Europäischen Forschungsrat entwickelt Gregor Leander neue Verschlüsselungsverfahren. Anders als üblich verlässt er sich dabei nicht nur auf das Prinzip von Versuch und Irrtum.

Sie beschützt uns jeden Tag und macht sich selten bemerkbar: die Kryptografie, also die Verschlüsselung von Informationen. Aus unserem digitalen Alltag ist sie nicht wegzudenken, denn würden Daten nicht durch mathematische Verfahren verschlüsselt werden, könnte jeder auf sie zugreifen. Die Inhalte von Chats würden genauso offenliegen wie die Daten unseres Online-Bankings. Durch die voranschreitende Digitalisierung müssen immer größere Datenmengen auf diese Weise gesichert werden. Dafür braucht es besonders starke kryptografische Lösungen, die in der Praxis schnell und effizient arbeiten und gleichzeitig absolut sicher sind. Dieser Herausforderung widmet sich Prof. Dr. Gregor Leander von der Fakultät für Informatik und dem Horst-Görtz-Institut für IT-Sicherheit an der Ruhr-Universität Bochum in seinem Forschungsprojekt „SymTrust".

Der Europäische Forschungsrat ERC fördert seine Arbeiten mit einem Advanced Grant, der mit 2,5 Millionen Euro für fünf Jahre dotiert ist. Das Projekt startet im Sommer 2023.

Vertrauen in die Sicherheit

„In den vergangenen Jahrzehnten lag der Hauptfokus bei den Verschlüsselungen auf der Schnelligkeit, statt auf guten Sicherheitsargumenten", erklärt Gregor Leander. Er widmet sich in seiner Forschung der Symmetrischen Kryptografie. Dieses traditionelle System, das es schon seit Cäsar gibt, arbeitet mit einem gemeinsamen geheimen Schlüssel, den nur Empfänger und Sender kennen, um sicher versenden und dechiffrieren zu können. Auf digitalen Geräten geschieht dies im Hintergrund, sodass Anwender*innen davon nichts mitbekommen. „Symmetrische Kryptografie, neben der asymmetrischen Kryptografie, findet sich heutzutage überall, da im Prinzip alles, jede Internetverbindung, jeder Autoschlüssel und jedes Handygespräch, verschlüsselt ist." Gängige Verfahren wie der Advanced Encryption Standard (AES) gelten heute zwar als absolut sicher, weil sie langjährig erforscht wurden und trotzdem nicht gebrochen wurden. „Es muss aber immer gute Sicherheitsargumente geben, warum die Verschlüsselungen sicher sind. Die Annahme ‚Es ist sicher, weil es noch niemand gebrochen hat' ist aus meiner Sicht kein gutes Argument. Wir können es uns in dieser digitalen Welt nicht leisten, dass unsere Kryptografie großflächig kaputtgehen könnte", argumentiert Gregor Leander.

Deshalb möchte er in seinem ERC Advanced Grant SymTrust daran arbeiten, neue symmetrische Verfahren zu entwickeln, die von Anfang an auf guten Sicherheitsargumenten basieren und innerhalb ihrer Implementierung, also der praktischen Anwendung, effizient und schnell arbeiten können. „Für mich ist es eine große Ehre, dass der European Research Council mich für dieses High-risk/high-gain-Projekt unterstützt. Ich freue mich darauf, dadurch fünf Jahre meines Lebens mit guten Doktorandinnen und Doktoranden sowie Postdocs an so einem spannenden Thema forschen zu können."

Neue Herangehensweise in der Entwicklung von Chiffren

Um seine Ideen umzusetzen, will der Inhaber des Lehrstuhls für Symmetrische Kryptographie anders an die Entwicklung von Chiffren, also der Verschlüsselung, herangehen, als es bisher üblich ist. Momentan unterliegt der Designprozess einem Trial-and-Error-Prinzip: Die Chiffre wird entworfen, in die technische Umgebung unter dem Aspekt der Effizienz eingebaut, und erst dann wird versucht, sie anzugreifen. Falls dies gelingt, wird noch einmal nachjustiert und der Prozess beginnt von vorn. Dies kann unter Umständen Jahre dauern – Zeit, die in modernen Entwicklungsprozessen im Prinzip nicht vorhanden ist. Deshalb besteht in der Industrie immer wieder die Problematik, dass die Sicherheit zu kurz kommt. „Ich will Chiffren designen, die heutigen und zukünftigen Anwendungen dienen können und mit Sicherheitsargumenten ausgestattet sind, denen man direkt vertrauen kann, ohne jahrelang darauf zu warten“, so Leander. Dazu muss er, zusammen mit seinem Team, aktuell bestehende Chiffren genauestens erforschen und sich mit den Bedingungen der Kryptoanalyse, der Wissenschaft des Brechens der Chiffren, intensiv auseinandersetzen.

Die daraus gewonnenen Erkenntnisse sollen dazu dienen, schließlich ein neues Konzept für die Symmetrische Kryptografie zu entwickeln, das für die Industrie sowie die Wissenschaft neue Maßstäbe bei der Verschlüsselung von Informationen setzen will.

Zur Person

Gregor Leander studierte Mathematik an der Universität Bremen und promovierte 2004 an der Ruhr-Universität Bochum. Mit einer Förderung vom Deutschen Akademischen Austauschdienst ging er 2006 als Postdoktorand an die Universität von Toulon, Frankreich, von wo aus er 2008 als Assoziierter Professor an die Technische Universität von Dänemark in Lyngby wechselte. 2012 kam er an die Ruhr-Universität zurück, wo er 2015 eine Heisenberg-Professur besetzte. Er ist Principle Investigator im Exzellenzcluster CASA, kurz für „Cyber Security in the Age of Large-Scale Adversaries”, und dort Dean der Graduate School. Zwei von ihm entworfene Verschlüsselungen (Present und Skinny) sind ISO-zertifiziert. Seine Forschungsarbeit wurde bereits zweimal mit einem Best Paper Award gewürdigt, und er gewann außerdem 2010 den ersten Platz beim Deutschen IT-Sicherheitspreis. Den Lehrstuhl für Symmetrische Kryptographie an der Fakultät für Informatik hat er seit 2022 inne.

contact for scientific information:

Prof. Dr. Gregor Leander
Lehrstuhl für Symmetrische Kryptographie
Fakultät für Informatik
Ruhr-Universität Bochum
Tel.: +49 234 32 28402
E-Mail: gregor.leander@ruhr-uni-bochum.de

Gregor Leander wird mit einem Advanced Grant des Europäischen Forschungsrats ausgezeichnet.
© Michael Schwettmann