hoch3 FORSCHEN

Das Medium für Wissenschaft

Herbst 2020

TECHNISCHE UNIVERSITÄT DARMSTADT

Impressum

Herausgeber
Die Präsidentin
der TU Darmstadt

Redaktion Stabsstelle
Kommunikation und Medien
der TU Darmstadt:
Jörg Feuck (Leitung, V.i.S.d.P.)
Ulrike Albrecht (Grafik Design)
Patrick Bal (Bildredaktion)

Titelbild Im Merck Lab an der TU werden vereinfachte Diagnostik-Methoden entwickelt; Bild: Katrin Binner

Druck Druckerei Petzold GmbH, Darmstadt
gedruckt auf 100 g/m²
PlanoScript, FSC-zertifiziert

Auflage 5.000 **Nächste Ausgabe**
15. Dezember 2020

Leserservice presse@
tu-darmstadt.de

ISSN 2196-1506

Möchten Sie die nächste Ausgabe der hoch³FORSCHEN gerne in digitaler Form erhalten? Dann senden Sie bitte eine E-Mail an presse@tu-darmstadt.de

__ 1 Mobilität: Was Bahnreisende wissen wollen __ 2 Schnittstelle: Informatik trifft Friedens- und Konfliktforschung __ 3 Diagnostik: Multiresistente Keime eindämmen __ 4 Kryptografie: Wettlauf gegen den Riesen-Codeknacker

Informatik für den Frieden

Das PEASEC-Team forscht unter anderem zu resilienten IT-basierten kritischen Infrastrukturen.

Er forscht und lehrt an der Schnittstelle zwischen Informatik und Friedens- und Konfliktforschung. Was IT im Krieg und für den Frieden bewirken kann erklärt Professor Christian Reuter im Gespräch.

Abbildung: Hessen schafft Wissen – Jürgen Kneifel

Professor Christian Reuter

Herr Professor Reuter, der Wissenschaftsrat mahnt eine strukturelle Weiterentwicklung der naturwissenschaftlich-technischen Friedens- und Konfliktforschung in Deutschland an. Wie sind wir hierzulande aufgestellt?

Im Vergleich zur politikwissenschaftlichen Friedens- und Konfliktforschung deutlich weniger gut. Früher hatte dies eine höhere Bedeutung. Schon in den 1950er und 1960er Jahren haben sich Naturwissenschaftler und Naturwissenschaftlerinnen mit Dual-Use-Fragen beschäftigt, also zum Beispiel überlegt, was sie dazu beitragen können, dass Atomkraft nur für die Energieversorgung genutzt wird und nicht auch für die Herstellung waffenfähigen Materials. Heute ist diese Forschung an den deutschen Universitäten zu wenig vertreten. Strukturell, das heißt dauerhaft verankert, ist sie im Moment nur am Carl Friedrich von Weizsäcker-Zentrum der Universität Hamburg und bei uns an der TU Darmstadt. Dabei sind diese Themen aktueller denn je. Es ist mitnichten alles friedlich geworden. Ganz im Gegenteil: In Syrien werden Chemiewaffen eingesetzt, internationale Verträge über die Abrüstung von Langstreckenraketen werden gerade gekündigt. Und natürlich stehen wir im Cyber-Raum ganz neuen Herausforderungen gegenüber.

Welche Bedeutung spielen Cyber-Kriege und Cyber-Streitkräfte inzwischen?

Schädliche Aktivitäten zwischen den Staaten im Cyberspace werden gerade Normalität und Cyber-Streitkräfte sind neben den Boden-, Luft,- und See-streitkräften und den Aktivitäten im Weltraum zu einer neuen Säule der Kriegsführung geworden. Viele Staaten und Bündnisse rüsten ihre Cyber-Kapazitäten auf. Das gilt für die USA ebenso wie für die NATO oder Einzelstaaten wie Deutschland. Überall fließen Geld und Ressourcen in diesen Bereich und es werden neue Einheiten und Befugnisse geschaffen.

Was ist überhaupt eine Cyber-Waffe?

Jedenfalls nichts, was wir aus Star Wars-Filmen kennen. Das Ganze ist viel subtiler. Meistens handelt es sich um Sicherheitslücken in Software und Hardware, verbunden mit Code, um diese auszunutzen. Solche Lücken werden immer wertvoller. Wer sie für kriegerische Zwecke missbrauchen will, meldet sie nicht dem Hersteller, sondern sammelt sie für das eigene Waffenarsenal. Das exklusive Wissen über solche Hintertüren wird zum kriegsentscheidenden Vorteil. Die, die schon länger im Cyberspace aktiv sind, nutzen ihn, um in gegnerische IT-Systeme einzudringen. Das gefährdet nicht nur militärische, sondern auch zivile Systeme – zum Beispiel, wenn nicht nur der Raketenstützpunkt ins Visier gerät, sondern auch die Energieversorgung.

Kann man solche feindlichen Aktivitäten zurückverfolgen?

In der Regel können wir sie nicht zuordnen. Wenn irgendjemand eine Rakete abschießt, sieht man das auf Satellitenbildern. Der Hackerangriff auf die deutsche Bundesregierung im Dezember 2017 dagegen ist bis heute technisch nicht einwandfrei nachvollziehbar. Oft weiß man gar nicht, ob es sich einfach nur um kriminelle Aktivitäten handelt oder um Spionage – die zwar strafrechtlich verfolgt werden kann, aber keinen Kriegsfall auslösen würde – oder ob in Zusammenarbeit mit transnationalen Akteurinnen und Akteuren wirklich ein zwischenstaatlicher Konflikt provoziert werden soll. Es verschwimmt alles. Wir beobachten eine gefährliche Normalisierung von konstanten schädlichen Aktivitäten und von hybriden Konflikten. Das fördert nicht unbedingt das Vertrauen zwischen den Staaten.

Kontakt

Wissenschaft und Technik für Frieden und Sicherheit (PEASEC)
Prof. Dr. Christian Reuter
Telefon: 06151/16 – 20941
E-Mail: reuter@peasec.tu-darmstadt.de
https://peasec.de

Abbildung: shock/stock.adobe.com

Sie haben das Thema „Dual-Use“ angesprochen. Was können Sie in der Informatik tun, damit neue, digitale Technologien nicht für die Kriegsführung missbraucht werden?

Es geht hier nicht nur um Technikfolgenabschätzung oder die Absicherung von Infrastrukturen. Es geht vor allem auch um eine bewusste Technikgestaltung. Wir müssen Software von Anfang an so entwickeln, dass es möglichst wenig missbräuchliche oder kriegerische Nutzungsmöglichkeiten gibt. Gerade in der Informationstechnologie ist die Dual-Use-Frage aber eine riesige Herausforderung. Denn Software kann immer noch relativ einfach verändert und für andere Zwecke als den ursprünglich gedachten adaptiert werden.

An Ihrem Fachgebiet arbeiten Informatiker und Informatikerinnen mit Friedens- und Konfliktforschenden zusammen. Wie läuft das in der Praxis ab?

Wir verorten uns dort, wo beide Disziplinen sich inhaltlich überlappen. Wir bedienen uns einerseits der Methoden der empirischen Sozialforschung und analysieren zum Beispiel die Rolle neuer Technologien für Frieden und Sicherheit. Da geht es um Fragen wie: Wie werden soziale Medien in Konfliktlagen genutzt? Welche Dynamiken entstehen dort? Welche Narrative gibt es, die Meinungen manipulieren? Darauf aufbauend entwickeln wir dann technische Lösungen, die Eskalationen wie sogenannte Information Warfare verhindern. Wir haben zum Beispiel „Trusty Tweet“ entwickelt, ein Plugin für Browser, das Indikatoren transparent macht, die auf Fake News hindeuten. Wir arbeiten auch an Software, die Social-Media-Daten analysiert, um Missbrauch wie das Tracking von Personen von Anfang an einzudämmen.

Ich stelle mir eine solche kontinuierliche interdisziplinäre Zusammenarbeit sehr voraussetzungsvoll vor.

Ja. Sie setzt voraus, dass man ein vertieftes Verständnis für den jeweils anderen Bereich entwickeln kann. Aber nicht nur das. Wir müssen gemeinsam die Problemstellungen komplett durchdringen, um uns klar zu werden, auf welche konkreten Punkte wir uns fokussieren wollen. Es ist nicht so, dass die technischen Fragestellungen am Anfang stehen. Ausgangspunkt ist immer ein Defizit, welches zunächst genauer analysiert werden muss, um darauf aufbauend mögliche technische Lösungen zu entwickeln, die der Gesellschaft nutzen. Gleichzeitig müssen wir es schaffen, in unserer jeweiligen Fachwelt Akzeptanz zu finden. Denn wir wollen unsere Ergebnisse natürlich auf höchstem Niveau in die einzelnen Disziplinen einbringen, damit wir mit unserer Forschung dort sichtbar werden und andere darauf aufbauen können. Da muss man dann meistens noch einmal den Extra-Meter gehen.

Und was würden Sie gerne in Ihrer eigenen Fachwelt bewegen?

Als Informatiker und Informatikerinnen haben wir heute praktisch Einfluss auf das ganze Leben. Deswegen möchte ich dafür sensibilisieren, dass unsere Arbeit auch Schaden anrichten kann und dass wir mehr auf eine werteorientierte Gestaltung achten müssen, bei der nicht nur monetäre Aspekte eine Rolle spielen. Software kann oftmals unbeabsichtigt Entwicklungen in die falsche Richtung treiben. Also müssen wir lernen, aktive Entscheidungen zu treffen und schon während der Softwareentwicklung Weichenstellungen vornehmen, zum Beispiel bestimmte Nutzungsarten ausschließen oder bestimmte Module nur verschlüsselt bereitstellen. Jeder und jede sollte hierfür ein Bewusstsein entwickeln.

Das Interview führte Jutta Witte. Sie ist Wissenschaftsjournalistin und promovierte Historikerin.

Hintergrund:

Prof. Dr. Christian Reuter ist Leiter des 2017 an der TU Darmstadt geschaffenen Fachgebiets „Wissenschaft und Technik für Frieden und Sicherheit“ (PEASEC). Er gehört dem Fachbereich Informatik und im Rahmen einer Zweitmitgliedschaft auch dem Fachbereich Gesellschafts- und Geschichtswissenschaften an. Das PEASEC-Team forscht zu den Schwerpunktthemen „Sicherheitskritische Mensch-Computer-Interaktion“, „IT für Frieden und Sicherheit“ sowie „Resiliente IT-basierte (kritische) Infrastrukturen“. Das Fachgebiet ist eng verflochten mit dem Profilbereich Cybersicherheit der TU Darmstadt sowie mit dem am Forum Interdisziplinäre Forschung (FiF) der TU Darmstadt verankerten multi- und transdisziplinären Netzwerk IANUS.

https://peasec.de/2020/it-frieden

Aktuelle Publikation:
„Towards IT Peace Research“:
https://peasec.de/2020/towards-it-peace-research

Diagnostik aus dem Drucker

Im Merck Lab an der TU Darmstadt haben Forscher von Merck und der TU die Diagnostik von bakteriellen Infektionskrankheiten vereinfacht. Damit wollen sie ein globales Problem eindämmen: die Zunahme von multiresistenten Keimen, gegen die keine Antibiotika mehr helfen.

Von Uta Neubauer

„So viel wie nötig, so wenig wie möglich" sollte das Motto bei der Verwendung von Antibiotika lauten. Doch danach wird oft nicht gehandelt. Die Folge: Bei immer mehr krankmachenden Bakterien versagen die einst als Wunderwaffe gefeierten Medikamente. Vor allem in Kliniken sind multiresistente Keime mittlerweile ein gefürchtetes Problem. Sie führen zu Wundinfek-tionen, Blutvergiftungen oder anderen Krankheiten, die sich nur schwer oder gar nicht behandeln lassen.

„Laut Hochrechnungen werden schon im Jahr 2050 mehr Menschen an Infektionen mit resistenten Keimen sterben als an Krebs", sagt Dieter Spiehl, Forscher im Merck Lab an der TU Darmstadt. Neben dem überbordenden Einsatz von Antibiotika in der Massentierhaltung kritisiert er die gängige Verschreibungspraxis in der Humanmedizin. Bei einer Patientin mit einer Blasenentzündung etwa werde in der Regel nicht untersucht, welche Bakterienart den Infekt verursacht. Meist stecken Kolibakterien dahinter, manchmal aber auch Staphylokokken oder andere bakterielle Erreger. Das könnte man testen – klassischerweise mit einer Kultur in der Petrischale – und dann ein spezifisches Mittel verordnen. Doch nur Kliniken führen solche Analysen standardmäßig durch. „Für niedergelassene Ärzte ist die Untersuchung zu aufwendig und teuer. Sie verordnen stattdessen lieber Breitbandantibiotika", bemängelt Spiehl. Solche Präparate bekämpfen verschiedenste Erreger, allerdings auch harmlose körpereigene Bakterien. Das führt nicht nur zu unerwünschten Nebenwirkung, sondern befördert auch die Zunahme von resistenten Keimen. Denn immer, wenn Antibiotika eingesetzt werden, entwickeln die Bakterien Überlebensstrategien. Die widerstandsfähigsten überleben und breiten sich weiter aus.

„Die Tests sind so einfach und ohne Hightech-Laborausstattung durchführbar"

Mit vereinfachten diagnostischen Werkzeugen wollen die Forscher des Merck Lab das Problem jetzt eindämmen. „Wir möchten die klassische Petrischale durch Testkarten ersetzen", erläutert Gerhard Schwall vom Darmstädter Wissenschafts- und Technologieunternehmen Merck, der das Merck Lab an der TU leitet. Petrischalen seien relativ groß und mit Nährmedien gefüllt nur begrenzt haltbar. Die Anzucht einer Kultur erfordere zudem mikrobiologisch ausgebildetes Fachpersonal. In der Lebensmittelproduktion, in der Bakteriennachweise zur Routine zählen, haben sich daher schon alternative Analysenwerkzeuge etabliert: Testkarten mit aufgedruckten Nährmedien. Sie können trocken, ungekühlt und platzsparend gelagert werden. Dieses Konzept haben Spiehl und seine Kollegen auf die medizinische Diagnostik übertragen.

Die im Merck Lab entwickelten Testkarten identifizieren nicht nur Bakterien, sondern erkennen zudem Antibiotika-Resistenzen. Ihre Anwendung ist denkbar einfach: Ein Labor- oder Praxismitarbeiter tropft die Patientenprobe, zum Beispiel etwas Urin, auf das Kärtchen, deckt es mit einer Schutzfolie ab und legt es über Nacht in einen Wärmeschrank. Die bakteriellen Krankheitserreger vermehren sich und bilden – wie beim Standardtest in der Petrischale – Bakterienkolonien, die mit bloßem Auge zu erkennen sind. Das Testfeld enthält verschiedene Nachweisreagenzien, sodass sich beispielsweise Kolibakterien als rote Punkte zeigen, während sich Staphylokokken-Kolonien grün färben. Zwecks Resistenztestung befinden sich auf den Testkärtchen zudem verschiedene Antibiotika. Vermehren sich die Bakterien in einem derart präparierten Bereich, ebenfalls zur erkennen an einer Färbung des Feldes, bedeutet das: Achtung, dieses Antibiotikum hilft nicht gegen den Krankheitserreger!

Bei der Herstellung der Testkarten kommen verschiedene Druckverfahren zum Einsatz: Mit einer dickflüssigen Tinte, die das Nährmedium sowie Farbstoffe für den Bakteriennachweis enthält, druckt eine Siebdruckmaschine das Testfeld auf eine Folie. Hier wird später die flüssige Probe

Kontakt
Projektleiter
Merck Lab @ TU Darmstadt
Dr. Gerhard Schwall
E-Mail:
gerhard.schwall@merckgroup.com
Dr.-Ing. Dieter Spiehl
E-Mail:
spiehl@idd.tu-darmstadt.de
https://bit.ly/32pD7fG

aufgetropft. Damit sie nicht über das Feld hinausläuft, versieht ein 3D-Drucker den Umriss des Testfeldes mit einem Rand aus Kunststoff. Für die Resistenztestung werden verschiedene Antibiotika tröpfchenweise im Inkjet-Verfahren an bestimmten Positionen auf das Testfeld gedruckt. Spezielle Druckstrategien sorgen dafür, dass sich die Antibiotika beim Aufbringen der flüssigen Probe nicht beliebig auf dem Testfeld verteilen oder gar vermischen. Kurze Legenden und Vergleichsfelder für die Auswertung lassen sich ebenfalls direkt auf die Karte drucken. Zum Schluss wird das System mit einer durchsichtigen Schutzfolie versehen, die zum Auftropfen der Probe hochgeklappt wird. „Etwa 1500 Testkarten haben wir schon gedruckt und verwendet“, schätzt Spiehl.

Als promovierter Maschinenbauer kannte sich Spiehl mit Drucktechniken bereits bestens aus. In seiner Doktorarbeit hat er sich mit dem Drucken von Elektronik beschäftigt, dem damaligen Fokus des Merck Lab. Parallel zu dem jetzigen Projekt leitet er eine Forschungsgruppe am Institut für Druckmaschinen und Druckverfahren der TU. Mit Infektionskrankheiten und ihrer Diagnostik machte er sich in dem multidisziplinären Team aus Biologen und Medizinern schnell vertraut. Drei Jahre lang tüftelten er und seine Kollegen am Design und der Fertigung der Testkarten. Das Ergebnis kann sich sehen lassen: „Wir haben Prototypen für verschiedene Anwendungen hergestellt und die Machbarkeit des Konzepts gezeigt“, sagt Spiehl.

„Die Tests sind so einfach und ohne Hightech-Laborausstattung durchführbar, dass sie sich besonders für kleine, wenig automatisierte Labore eignen, auch in Entwicklungsländern“, betont Laborleiter Schwall. In den ärmsten Regionen der Welt ist das Problem gravierend: Unter bakteriellen Infektionen leiden dort deutlich mehr Menschen, zugleich werden Antibiotika oft unkontrolliert verwendet und damit Resistenzen gefördert. „Mit Ärzten und Laboranten aus europäischen und afrikanischen Ländern haben wir deren Bedürfnisse bezüglich vereinfachter Diagnostik besprochen“, sagt Spiehl. Das Interesse aus Ländern wie Nigeria und Simbabwe sei groß: „Wir hatten schon Versuchsreihen mit zwei Laborketten in Afrika geplant, doch dann kam die Corona-Pandemie und wir mussten das Vorhaben auf unbestimmte Zeit verschieben.“

An der Frankfurter Universitätsklinik wurden die neuen Diagnostikwerkzeuge schon getestet. Hunderte Proben, unter anderem von Patienten mit Harnwegsinfekten, wurden dort mit den Testkarten aus dem Merck Lab untersucht, immer parallel zum Standardverfahren in der Petrischale. „Schritt für Schritt haben wir unser System optimiert und letztendlich gezeigt, dass es funktioniert“, freut sich Spiehl. Gemeinsam mit Merck prüfen er und seine Kollegen derzeit die kommerzielle Nutzung. Für die TU-Forscher endet das Projekt dieses Jahr. Bleibt zu hoffen, dass die Testkarten zügig bis zur Marktreife weiterentwickelt werden und so einen wertvollen Beitrag im Kampf gegen antibiotikaresistente Keime leisten.

Die Autorin ist Wissenschaftsjournalistin und promovierte Chemikerin

Mit verschiedenen Druckverfahren werden im Merck Lab an der TU Testkarten hergestellt, die zukünftig eine vereinfachte Diagnostik von Infektionskrankheiten ermöglichen.

Abbildung: Katrin Binner

Wettlauf gegen den großen Codeknacker

Quantencomputer könnten schon in zehn Jahren die im Netz gängigen Verschlüsselungen knacken – auch rückwirkend. Die Darmstädter Kryptografin Dr. Juliane Krämer hält mit Mathematik dagegen.

Abbildung: Ralf Werner

‚Post-Quantum-Kryptografie ist das Forschungsthema von Juliane Krämer, Mathematikerin und Informatikerin an der TU Darmstadt.

Von Christian J. Meier

„Versetzen Sie sich in die nahe Zukunft und stellen Sie sich eine Website vor, auf der jeder Ihre WhatsApp-Kommunikation von heute sehen könnte“, sagt Dr. Juliane Krämer. „Ab wann würde Sie das nicht mehr stören? In einem Jahr? In zehn Jahren?“, fragt die Forscherin aus dem Profilbereich CYSEC der TU Darmstadt. Krämer verbindet die Fragen mit einer Warnung: Schon in einigen Jahren könnte es einen Quantencomputer geben, der die heute im Internet gängigen Verschlüsselungen knackt. Im Sonderforschungsbereich CROSSING entwickelt die Kryptografin neue Methoden, die dem Codeknacker trotzen, so genannte Post-Quanten-Kryptografie. Sie meint, je nach Schutzbedürfnis müsse man sich schon heute gegen den Zukunftsrechner wappnen.

Kontakt

Forschungsgruppe
Quantum and Physical attack resistant Cryptography (QPC)
Dr. Juliane Krämer
Telefon: 06151/16–20662
E-Mail: juliane@qpc.tu-darmstadt.de
www.informatik.tu-darmstadt.de/qpc

Die bedrohten Methoden schützen vor Lauschern und erzeugen digitale Signaturen, ohne die Online-Banking oder Softwareupdates nicht vertrauenswürdig wären. Um Daten zu verschlüsseln, verwandelt der Sender sie in einen Zeichensalat, den nur der Empfänger wieder entwirren kann. Damit die beiden keinen geheimen Schlüssel tauschen müssen, verwendet man so genannte „asymmetrische Kryptoverfahren“. Der Empfänger, etwa eine Bank, stellt den Schlüssel öffentlich zur Verfügung. Damit kann der Sender seine Nachricht an die Bank leicht verschlüsseln. Der öffentliche Schlüssel kann jedoch nicht zum Entschlüsseln verwendet werden. Dafür besitzt allein der Empfänger einen „privaten Schlüssel“. Verwirklicht wird dies mit einer Art mathematischem Drehkreuz. Dieses lässt sich in die eine Richtung widerstandslos durchschreiten (das Verschlüsseln per öffentlichem Schlüssel). In der anderen Richtung jedoch sperrt es. Nur der Besitzer hat einen Schlüssel, der den Sperrmechanismus öffnet (das Entschlüsseln mit dem privaten Schlüssel) und ihn in der gesperrten Richtung passieren lässt. Das digitale Signieren funktioniert genauso, nur mit umgekehrtem Informationsfluss: Der Sender erstellt mit seinem privaten Schlüssel die elektronische Unterschrift. Der Empfänger kann deren Echtheit mit dem öffentlichen Schlüssel prüfen.

Das heute meistgenutzte „Drehkreuz“ arbeitet mit sehr großen Primzahlen. Die Multiplikation zweier Primzahlen ist leicht. Der umgekehrte Weg, das Produkt in seine Primfaktoren zu zerlegen, aber ist derart schwer, dass selbst Supercomputer dafür Jahrzehnte bräuchten. Das Produkt kann jede Person als öffentlichen Schlüssel zum Verschlüsseln nutzen. Nur der Empfänger kennt die Primfaktoren, die er als privaten Schlüssel verwendet. Dieses so genannte RSA-Verfahren und verwandte Methoden sichern täglich milliardenfach die Kommunikation im Netz. Doch damit könnte es auf einen Schlag vorbei sein, sobald ein leistungsstarker Quantencomputer bereitstünde. Denn ausgerechnet die derzeit genutzten digitalen Drehkreuze sind für ihn keine. Er führt die Rückwärtsrechnung blitzschnell durch.

Allerdings wird der Quantenrechner kein Allrounder sein. Es sind erst wenige Probleme bekannt, deren Lösung er radikal beschleunigen wird. Viele Aufgaben, so die Meinung unter Forschenden, wird er kaum oder gar nicht schneller lösen als ein normaler Computer. Dazu gehören andere mathematische Drehkreuze als die derzeit in der

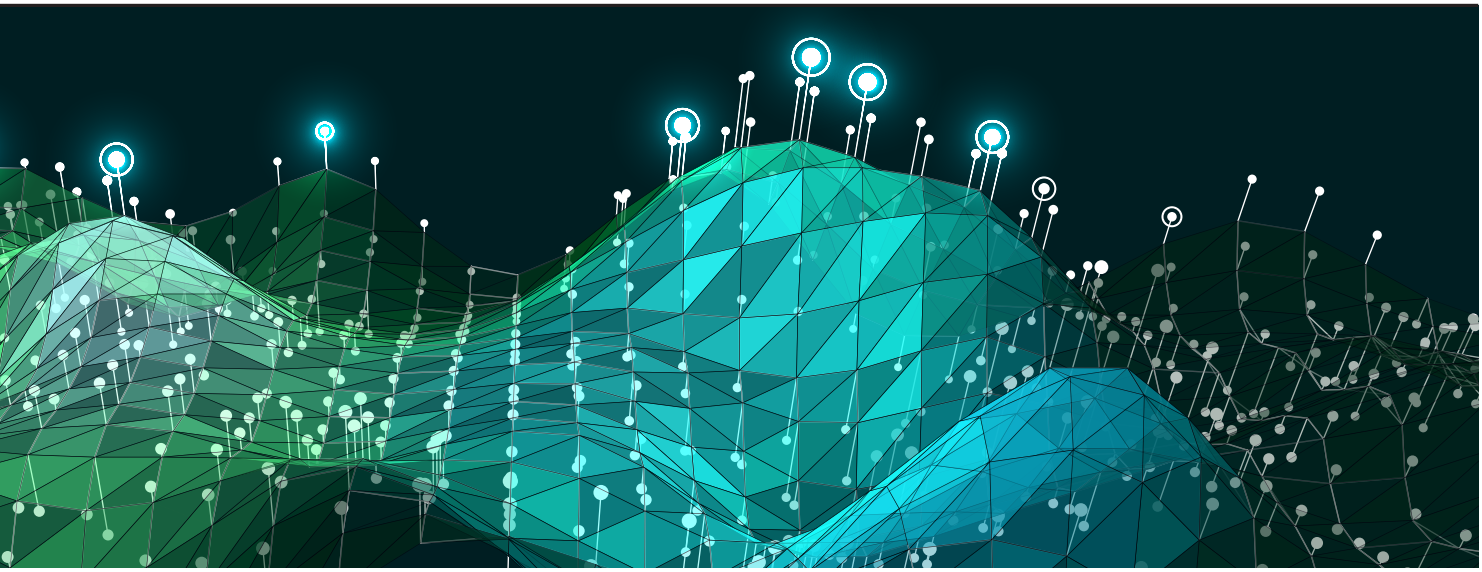

Abbildung: Adobestock

Juliane Krämer forscht an neuen Post-QuantenVerfahren zum Schutz gegen Quantencomputer der Zukunft.

Kryptografie genutzten. Spezialistinnen wie Juliane Krämer entwickeln daraus neue Kryptoverfahren. „Die Post-Quanten-Kryptografie ist ein sehr aktives Forschungsfeld“, sagt die Mathematikerin und Informatikerin. Sie selbst erforscht die so genannte „gitterbasierte Kryptografie“. Unter „Gitter“ versteht die Mathematik einen Raum, gefüllt mit regelmäßig angeordneten „Gitterpunkten“. Ein Bauzaun ähnelt einem Gitter mit zwei Dimensionen: Die Kreuzungen der Drähte bilden die Gitterpunkte. Mathematikern und Mathematikerinnen fällt es leicht, Gitter mit hunderten Dimensionen aufzuspannen, freilich nur als virtuelles Gebilde. Nun kann man einen zusätzlichen Punkt irgendwo zwischen die einzelnen Gitterpunkte setzen. Wegen der vielen Dimensionen kann es äußerst schwierig sein, den nächsten Gitterpunkt zu finden. Es kann aber auch leicht sein. Das hängt davon ab, wie das Gitter mathematisch beschrieben wird. In der Mathematik spricht man von einer „schlechten“ oder einer „guten“ Basis. Wird nun eine „schlechte Basis“ als öffentlicher Schlüssel und eine „gute“ als privater verwendet, hat man ein mathematisches „Drehkreuz“ gestaltet.

„Die Post-Quanten-Kryptografie ist ein sehr aktives Forschungsfeld.“

Bekannt sind dieses und ähnliche Probleme schon lange. „Doch welche Probleme sich in der Praxis als hochrelevant durchsetzen werden und welche nicht, muss sich erst noch zeigen“, sagt Krämer. Derzeit suchten Entwicklungs-Teams eine geeignete Balance zwischen Sicherheit und Effizienz der Verfahren. Die Forschenden spielen etwa mit unterschiedlichen mathematischen Darstellungen von Gittern. Mit einer davon, in Form von „Polynomen“, laufen die Rechenoperationen schneller. Doch die Schlüssel benötigen relativ viel Speicherplatz, was für mobile Anwendungen, etwa in Handys, ein Nachteil ist. „Es gibt kein Patentrezept für die Steigerung der Effizienz“, sagt Krämer. Kreativität sei gefragt.

Forschungs-Teams schaffen viele Methoden mit unterschiedlichen Vor- und Nachteilen in puncto Sicherheit und Effizienz. Die amerikanische Standardisierungsbehörde NIST hat 2016 zu einem Wettbewerb aufgerufen, für den rund 80 Vorschläge eingingen. Nach einer ersten Evaluierung blieben 29 Methoden. Die meisten davon sind gitterbasiert. Die NIST hat Schwächen der einzelnen Verfahren benannt und Nachbesserungen von den Autoren gefordert. „Die Methoden sind öffentlich“, erklärt Krämer. Fachkollegen und -kolleginnen finden Sicherheitslücken, die die Urheber dann stopfen. Inzwischen hat die NIST das Bewerberfeld weiter eingeschränkt. Unterdessen arbeitet Juliane Krämer unter anderem an Prüfverfahren, die möglichst sicherstellen sollen, dass neue Post-Quanten-Verfahren tatsächlich auch gegen Quantenrechner schützen. Eine absolute Sicherheit kann es allerdings nie geben, da die Unknackbarkeit stets auf Annahmen beruht, auch bei den aktuell genutzten Verfahren.

Bis die Standards für die Post-Quanten-Kryptografie feststehen, klafft eine Art Verschlüsselungs-Lücke, warnt Krämer. Während digitale Signaturen nur für den Moment sicher sein müssen, sollten verschlüsselte Daten es oft dauerhaft bleiben. Heute chiffrierte Daten könnte ein Quantenrechner in einigen Jahren knacken. Wer längerfristig auf der sicheren Seite sein will, sollte RSA und Co. schon heute nicht mehr nutzen, empfiehlt die Kryptografin. Etliche Verfahren seien durchaus einsatzbereit.

Der Autor ist Wissenschaftsjournalist und promovierter Physiker.

Links und Publikation:

Sonderforschungsbereich Crossing an der TU Darmstadt:
www.crossing.tu-darmstadt.de/crc_1119/index.en.jsp

Profilbereich Cybersicherheit (CYSEC) an der TU Darmstadt:
www.cysec.tu-darmstadt.de/cysec/index.de.jsp

Podcast:
https://www.hessen-schafft-wissen.de/podcast/Juliane-Kraemer

Aktuelle Publikation: Krämer, Struck (2020): Encryption Schemes using Random Oracles: from Classical to Post-Quantum Security. PQCrypto, 2020, Paris, France

Schnelle Fakten

Wissenschaftler der TU Darmstadt beleuchten das Thema Fahrgastinformation in Zügen der DB Regio AG.

Von Astrid Ludwig

Diese Erfahrung ist Allgemeingut: Der gebuchte Zug ist pünktlich, aber voll, verspätet oder fällt wegen eines Hindernisses aus. Welche Informationen wünschen sich Berufspendler und Freizeitreisende im Regelbetrieb und bei Störfällen? Wann, wie und über welche Informationskanäle sollten in Regionalzügen und S-Bahnen diese Infos am besten bereitgestellt werden? Forscher der TU Darmstadt und der DB Regio AG haben im Rahmen der Innovationsallianz, welche die Universität und die Deutsche Bahn pflegen, untersucht, wie eine moderne, bedarfsgerechte und flexible Fahrgastinformation im Regionalverkehr aussehen sollte.

„Die Informationsmöglichkeiten halten nicht Schritt mit der aktuellen Digitalisierung und IT“, sagt Manfred Boltze, Professor und Leiter des Institutes für Verkehrsplanung und Verkehrstechnik an der TU Darmstadt. Die Züge sind oftmals alt, die Technik nicht auf dem neuesten Stand. Die bisherigen Formen visueller und akustischer Fahrgastinformation wirkten zunehmend überholt, statisch und bedingt durch lange Vertragslaufzeiten installierter Systeme wenig innovativ, so der Verkehrsplaner. Für ein neues Konzept, das insbesondere die Bedürfnisse der Zugreisenden aufgreift, haben die Forscher rund tausend Bahnkundinnen und -kunden befragt. Die Fragebögen wurden zusammen mit DB-Experten für Tagespendler und andere Reisende in Nahverkehrszügen im Rhein-Main-Gebiet entwickelt. Konkret wurde erhoben, wann sich Fahrgäste welche Informationen wünschen, wie die Lautstärke von Durchsagen geregelt sein sollte, wo Hinweise gut sichtbar platziert sein sollten und welche Fragen und Antworten beispielsweise im Störfall Vorrang haben. Wichtige Erkenntnis daraus: Der Informationsbedarf unterscheidet sich kaum bei Pendlern, Freizeitreisenden, Studierenden, älteren oder jüngeren Menschen. „Das hat uns überrascht. Wir hatten größerer Differenzen erwartet“, so Professor Boltze. Alle Gruppen wünschen sich danach in erster Linie Informationen über Pünktlichkeit, An- und Abfahrtszeiten, alternative Anschlüsse bei Verspätung oder Betriebsstörung. „Die harten Fakten, zeitnah, zuverlässig und leicht verständlich“, fasst Manfred Boltze zusammen.

Kontakt

Institut für Verkehrsplanung und Verkehrstechnik
Prof. Dr.-Ing. Manfred Boltze
Telefon: 06151/16 – 22500
E-Mail:
boltze@verkehr.tu-darmstadt.de
www.tu-darmstadt.de/verkehr
DB Regio AG
Dr.-Ing. Leif Fornauf
E-Mail:
Leif.Fornauf@deutschebahn.com

Fast die Hälfte der Befragten wünschen sich Informationen über die aktuelle Auslastung des Zuges und zwar bereits an der Station, an der sie auf den Zug warten. Knapp 60 Prozent wollen im Falle einer Fahrtunterbrechung weiterführende Informationen im Zug angezeigt oder angesagt bekommen. Generell ist Wissen über die betriebliche Situation gefragt; Infos zum Wetter, Nachrichten oder Werbung sind für die meisten Fahrgäste nebensächlich und uninteressant. Wichtig sind laut Boltze rechtzeitige und konsistente Informationen, sodass auf allen Informationskanälen identische Inhalte vorliegen und keine Verwirrung entsteht. Über 80 Prozent der Fahrgäste besitzen ein Smartphone mit installierter Reise-App, über 60 Prozent nutzen diese oft oder sogar bei jeder Reise. Und doch gaben über 30 Prozent an, dass sie ihr Wissen während der Fahrt hauptsächlich aus den Zugmedien beziehen.

Diese müssen daher aktuell, modern, gut sicht- und hörbar sein – auch für mobilitätseingeschränkte Personen. Möglichkeiten für eine umfassende, schnelle Information bieten nach Ansicht der TU-Forscher unter anderem Richtlautsprecher, Seitenscheibendisplays, Informationsstelen oder in den Zugabteilen installierte Zusatzdisplays, die freie Sitzplätze oder Gepäckfächer anzeigen.

Die Autorin ist Wissenschaftsjournalistin.

Weiterführende Informationen

Der Kurzbericht „Moderne Fahrgastinformation – Bedarfsgerecht, flexibel und innovativ unterwegs in Zügen des Regionalverkehrs“ wird in Kürze publiziert unter
https://www.verkehr.tu-darmstadt.de/vv/das_institut_ivv/
Über die Innovationsallianz TU Darmstadt und Deutsche Bahn:
https://bit.ly/2XXHlK4

Abbildung: Deutsche Bahn AG / Volker Emersleben

Das Institut für Verkehrsplanung untersucht, welche Informationen für Bahnreisende besonders wichtig sind.