Die Königin der Kryptografie

Im Internet einkaufen oder Passwörter benutzen wäre ohne die Arbeit von Shafi Goldwasser nicht möglich. Am Montag wird die Informatikerin in Berlin geehrt

Von Oliver Voss

Das Münzwurfrätsel hat Shafi Goldwasser nicht mehr losgelassen. Als sie angefangen hatte, Mathematik zu studieren, wurde die New Yorkerin mit dem Gedankenexperiment konfrontiert. Es geht darin um Alice und Bob, die sich gerade getrennt haben. Nun streiten sie darum, wer den Hund bekommt und wer das Auto. Ein Münzwurf soll die Fragen lösen, doch dabei gibt es ein Problem: Inzwischen leben sie getrennt in zwei verschiedenen Städten, doch wie können sie am Telefon darauf vertrauen, dass die Münze auch das anzeigt, was der andere behauptet?

Immer wieder hat sie darüber nachgedacht und fand einige Jahre später – sie war inzwischen von der Ostküste nach Berkeley in Kalifornien gezogen – eine Lösung für das Problem. Es handelt sich dabei um den „Zero-Knowledge-Beweis" – einen Beweis ohne Wissen. Damit kann jemand nachweisen, dass er eine geheime Information, wie beispielsweise ein Passwort, kennt, ohne dieses selbst preisgeben zu müssen. Stattdessen muss er eine Reihe Fragen beantworten, um zu beweisen, dass er die Lösung kennt, ohne sie selbst zu nennen. Das Ganze funktioniert mit komplexen mathematischen Funktionen. Goldwasser kam dabei zugute, dass ihre ursprüngliche Liebe der Zahlentheorie galt und sie erst im Laufe des Studiums die Informatik für sich entdeckte.

Für den „Zero-Knowledge-Beweis" und andere wissenschaftliche Leistungen hat Goldwasser neben verschiedenen anderen hochrangigen Auszeichnungen den Turing-Award erhalten, der als Nobelpreis der Informatik gilt. Sie ist dabei erst die zweite Frau, die den seit 1966 vergebenen Preis erhalten hat. An diesem Montag wird Goldwasser zudem vom Berliner Zuse-Institut in die „Hall of Fame of the Digital Age" aufgenommen.

Foto: Weizmann Institute of Science

Shafi Goldwasser erhielt den Turing-Award, den Nobelpreis der Informatik

Zu diesem Anlass wird sie einen Keynote-Vortrag auf der Konferenz „Digital Future Science Match" halten, die vom Tagesspiegel mitveranstaltet wird.

„Ihre Karriere umfasst viele wegweisende Arbeiten, die ganze Teilgebiete der Informatik initiiert haben", heißt es in der Begründung zur Verleihung des Turing-Preises. „Dazu gehören die Schaffung der theoretischen Grundlagen der modernen Kryptografie". Denn Goldwasser hat auch zahlreiche mathematische Beweise dafür geführt, ob und unter welchen Voraussetzungen Verschlüsselungen sicher sind. „Schon Julius Cäsar mag die Kryptografie benutzt haben, aber jetzt begannen wir endlich, sie zu verstehen", sagt US-Informatiker Charles Rackoff über ihre Arbeiten. Dabei beschäftigte sie sich beispielsweise mit Pseudozufallsgeneratoren oder Theorien zum Nachweis von Primzahlen, die für viele Verschlüsselungssysteme genutzt werden.

Heute kommen ihre theoretischen Arbeiten zigfach im Internet zum Einsatz. Wenn wir im Internet einkaufen und mit Kreditkarte bezahlen, werden beispielsweise die Kartendaten eingegeben und überprüft. Dabei erfährt der entsprechende Onlineshop oft aber nicht die Daten selbst, sondern nur eine Bestätigung dafür, dass sie stimmen. „Jedes Passwort, das wir eintippen, ist mit Techniken geschützt, die auf unserer Arbeit basieren", sagt Silvio Micali, mit dem Goldwasser in Berkeley gemeinsam viele wichtige Arbeiten erstellt hat und gemeinsam 2012 den Informatiker-Nobelpreis erhielt.

Doch ihre Arbeiten sind nicht nur elementar, wenn es heutzutage darum geht, für Sicherheit im Internet zu sorgen. Sie könnten auch die Privatsphäre der Zukunft sichern. Denn da Verschlüsselungssysteme auf mathematischen Verfahren beruhen, lassen sie sich mit diesen Methoden auch knacken. In der Regel ist es „nur" eine Frage der Rechenleistung, ob beziehungsweise wann sich ein Code entschlüsseln lässt. So ist die Entwicklung von Computern und Informatik wesentlich durch den Wettlauf zwischen Verschlüsselungssystemen und neuen Rechenmaschinen zur Dechiffrierung geprägt. Die Decodierung der Funksprüche der Nazis und deren Verschlüsselungsmaschine Enigma war beispielsweise eine der ersten großen Leistungen von Alan Turing, dem britischen Mitgründer der theoretischen Informatik.

Der nächste Durchbruch soll Quantencomputern gelingen, die viele der derzeit noch als sicher geltenden – weil mit schierer Rechenleistung nicht zu lösenden – Verschlüsselungssysteme knacken könnten. „Im Feld des Quantum-Computing sind neue Kryptografie-Verfahren notwendig, um den reibungslosen Ablauf einer vernetzten Gesellschaft zu garantieren", sagt Christoph Meinel, Direktor des Hasso-Plattner-Instituts in Potsdam. Experten wie Meinel gehen davon aus, dass viele der theoretischen Arbeiten von Goldwasser, die noch keine praktische Anwendung finden, die Grundlage bilden könnten, um in der Zukunft der Quantencomputer neue, noch sicherere Verschlüsselungsmethoden zu entwickeln.

Verschlüsselt. *Jedes Passwort, das wir in das Smartphone oder den Computer eintippen, ist mit Techniken geschützt, die auf den Arbeiten von Shafi Goldwasser und ihrem Team basieren.* Foto: iStock

HALL OF FAME

Digital-Pioniere

Aus Anlass des 75. Geburtstags des Computers, der 1941 in Berlin von dem Erfinder Konrad Zuse vorgestellt wurde, haben das Zuse-Institut und der **Tagesspiegel** 2016 die **„Hall of Fame of the Digital Age"** ins Leben gerufen. Die Mitglieder reichen vom Begründer der Informationstheorie John Shannon über den Spieltheoretiker John von Neumann, WWW-Erfinder Tim-Berners Lee bis hin zu Microsoft-Gründer **Bill Gates**. 2017 wurde Apple-Mitgründer Steve Wozniak aufgenommen. Nun kommt **Shafi Goldwasser** als 77. Mitglied hinzu. Porträts aller Mitgliedern unter: www.tagesspiegel.de/themen/digitale-pioniere/

SCIENCE MATCH

Digital-Konferenz

Die vom Tagesspiegel mitorganisierte Konferenz **„Digital Future Science Match"** findet anlässlich der Erfindung des Computers Z3 durch Konrad Zuse im Mai 1941 jedes Frühjahr in Berlin statt. Zur vierten Ausgabe werden am **14. Mai** im ehemaligen Kino Kosmos an der Karl-Marx-Allee etwa **1000 Gäste** aus Wissenschaft, Wirtschaft und Politik erwartet. Thematische Schwerpunkte in diesem Jahr sind **Big Data** und Artificial Intelligence, Cyber Security, Digital Decision Support und Self-determination in a **Networked Society**. Weitere Informationen unter: https://science-match.tagesspiegel.de/

Lieber Gründer als Berater

Die staatliche KfW-Förderbank bringt die Start-up-Szene in Bewegung – als Ankerinvestor für privates Kapital auch aus Berlin

Es sind junge Leute, deren Engagement Ingrid Hengster gefällt. Sie sitzt im Vorstand der bundeseigenen Förderbank KfW und ist für das inländische Fördergeschäft zuständig. Und damit auch für Gründer und Start-ups. An diesem Frühlingstag hört sie in einer trendigen Büroetage in der Speicherstadt in Hamburg fasziniert zu. Vor ihr steht Gunnar Froh und schwärmt von seinem Unternehmen als Teil der „neuen deutschen Automobilindustrie". Autos freilich werden bei „Wunder Car" nicht gebaut, dafür neue Mobilitätskonzepte entworfen, die bereits in Manila, der Hauptstadt der Philippinen, im indischen Bangalore und in Rio de Janeiro zum Alltag gehören. Ab Sommer auch in einer kleineren deutschen Stadt in Kooperation mit einem ÖPNV-Betreiber. Details verrät Froh noch nicht. Erste Projekte für Ridesharing – das Teilen von Plätzen in Privatautos über eine App – in Hamburg und Berlin waren kurz nach der Wunder-Gründung 2014 verboten worden.

Davon ist heute keine Rede mehr. Froh und seine Mitstreiter lassen sich nicht beirren. Mehr als zwei Millionen Fahrten habe man bereits vermittelt. Pendler bieten dabei freie Sitzplätze in ihren Autos zu festen Preisen über eine App an. An Wunder fließt eine Provision. In Hamburg tüfteln 55 Mitarbeiter aus 26 Ländern an der Weiterentwicklung der App. „Wir wollen bis 2020 in rund 20 Megastädten mit rund 300 Millionen Menschen vertreten sein", sagt Froh.

VW, Daimler, BMW und Co. kommen um neue Mobilitätskonzepte nicht herum, das weiß man bei Wunder. Mit zwei Herstellern gibt es bereits eine Kooperation. Investoren sind von dem Konzept angetan – wie Blumberg Capital oder Cherry Ventures aus Berlin, ein Fonds von Gründern für Gründer, wie Unternehmenschef Filip Dames sagt, der Zalando mit aus der Taufe gehoben hat. Die KfW hat in Cherry investiert und damit auch in Wunder.

Die KfW stößt zwei Milliarden Euro von privater Seite an

„Bei Risikokapital gibt es in Deutschland eine Lücke von 500 bis 600 Millionen Euro im Jahr. Die wollen wir gemeinsam mit dem Bundeswirtschaftsministerium schließen und zudem privates Kapital gewinnen", sagt Ingrid Hengster. 200 Millionen Euro hat die KfW bislang in 14 Venture-Fonds investiert. In den nächsten zehn Jahren sollen insgesamt zwei Milliarden Euro dazukommen. „Ein Ankerinvestor ist für einen Fondsinitiator von großer Bedeutung, deswegen ist es wichtig, dass sich die KfW in diesem Bereich betätigt", betont Christoph Stresing vom Bundesverband Deutscher Kapitalgesellschaften BVK. 400 Millionen von der KfW könnten weitere zwei Milliarden Euro von privater Seite für junge Gründer bewegen. „Das ist wichtig für die Zukunfts- und die Wettbewerbsfähigkeit des Standortes Deutschland."

Das Potenzial ist da, sagt auch Tobias Seikel, Geschäftsführer von Hanse Ventures. Gemeinsam mit Gründern baut er Firmen im Bereich Online und Mobile, hilft Gründern nicht nur bei der Finanzierung, sondern auch bei der Organisation, etwa bei Buchhaltung oder Raumsuche. Nach vier bis acht Jahren werden die Firmen verkauft. Auch bei Hanse Ventures ist die KfW mit im Boot. „Dass wir das nächste Facebook finden, ist unrealistisch", sagt Seikel. Aktuell gehören zum Portfolio ein Online-Küchenplaner, ein Serviceportal für Pflege und eine Beratungsplattform für Immobilienverkäufer.

Dass ein Mangel an Gründern herrscht, weil es für Hochschulabgänger gut bezahlte Jobs gibt, bestreiten Seikel und Cherry-Ventures-Chef Dames. „Viele junge Leute wollen gründen und selbstständig sein, statt bei Beratungsfirmen anzuheuern", sagt Seikel. Es gebe viele „hungrige" Gründer mit guten Ideen.

Die hatten 2010 auch die Gründer von Finanzcheck.de. Aus einem Vergleichsportal für Ratenkredite ist heute ein Onlinedienst auch für Auto- und Unternehmenskredite geworden. Gründer und Chef Moritz Thiele sagt, Finanzcheck nehme den Banken viel Arbeit ab, indem nur Kunden zu einem Geldhaus weitergeleitet würden, die passten. „Damit haben einige Banken bis zu 50 Prozent geringere Akquisitionskosten." Rund 230 Beschäftigte zählt Finanzcheck in Hamburg, Berlin und Braunschweig. Wurde 2012 pro Jahr ein Kreditvolumen von 27 Millionen Euro vermittelt, „so schaffen wir das heute in wenigen Tagen", sagt Thiele. 45 Millionen Euro wurden bislang in das Fintech investiert, auch von Action Capital Partners in München. Der Venture Fonds hat seit 1999 Geld in über 60 Unternehmen gesteckt. Auch mit Unterstützung der KfW. Rolf Obertreis