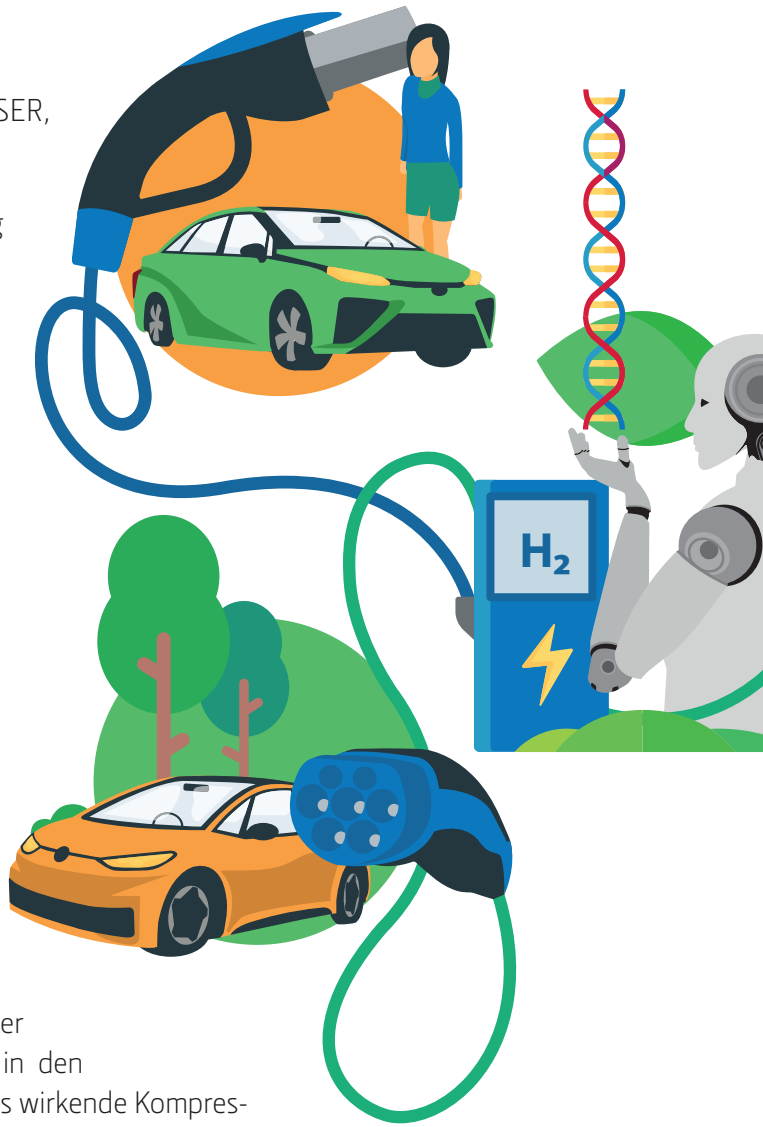


SEHR GEEHRTE LESERIN, SEHR GEEHRTER LESER,

WENN DIE Entwicklung der vergangenen Monate und Jahre uns eins gelehrt hat, dann dies: Die Bedeutung von Vernetzung und Digitalisierung wird in Zukunft noch zunehmen. Der technische Fortschritt wird eher noch einen Gang höher schalten als langsamer zu werden.

Die Themenschwerpunkte für dieses Sonderheft sind deshalb hoch relevant: Ob es um die Macht und Wirkungsweise der zehn bedeutendsten Algorithmen geht, die Vor- und Nachteile von Wasserstoff und Batterien für die Verkehrswende, die Zukunft der Authentifizierung im Internet, wie Quantencomputing funktioniert, oder die mangelnde Aussagekraft und die Datenschutz-Risiken von überall aus dem Boden sprießenden DNA-Analysen.

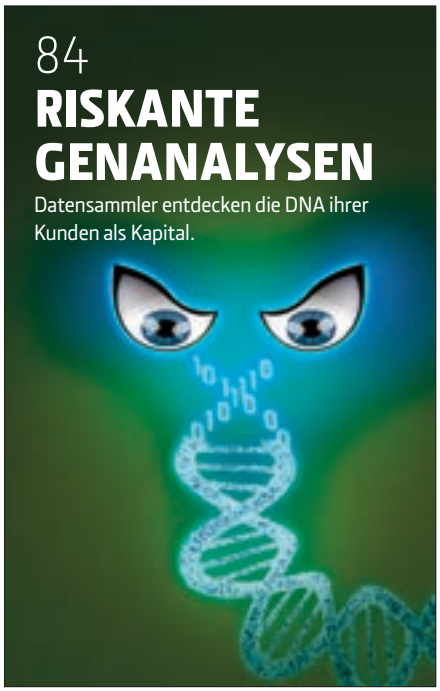
Was all diese Geschichten gemeinsam trägt, ist unsere Faszination für technische Durchbrüche, aber auch eine gesunde Skepsis gegenüber ihren gesellschaftlichen Auswirkungen. So wie in den Neunziger Jahren das auf den ersten Blick harmlos wirkende Kompressionsverfahren MP3 dafür sorgte, dass sich die Musikindustrie komplett neu erfinden musste. Heute müssen wir an dieser Stelle über generative neuronale Netze diskutieren – auch wenn es faszinierend ist, dass diese Software autonom Musik erschaffen kann.

Um diese Spannbreite an Themen zu stemmen, haben wir ein Experiment gewagt: Sie halten die erste gemeinsame Produktion der c't und der Technology Review in den Händen. Unsere Magazine hatten schon immer thematische Berührungspunkte. Jetzt haben wir unser Know-how zusammengelegt. Aus unserer Sicht ist dieses Experiment gelungen. Wir hoffen, Sie schließen sich diesem Urteil an.

Jo Bager

Dr. Wolfgang Stieler

INHALT



ALGORITHMEN

E-MOBILITÄT

DIGITALE MEDIZIN

SECURITY

QUANTENCOMPUTER

5G-NETZE

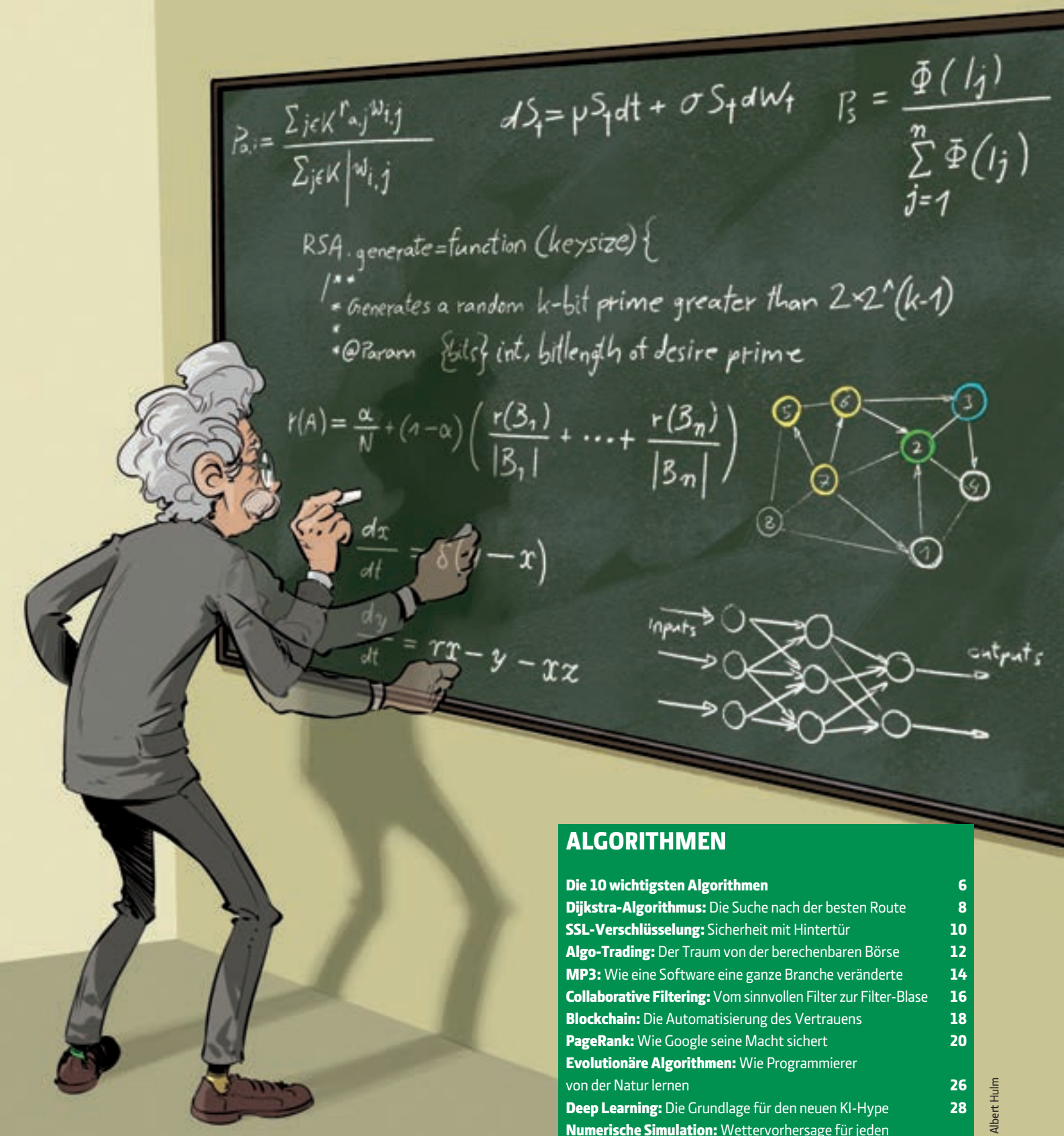


Illustration: Albert Hulm

ALGORITHMEN

Die **10 wichtigsten** Algorithmen

Wer hat Angst vorm Rechenwerk? Die Sorge vor einer Übermacht der Algorithmen beschäftigt mittlerweile Politik und Öffentlichkeit. Da kann etwas Grundwissen über ihre Funktion nicht schaden.

VON WOLFGANG STIELER

Sie sind überall, und sie sind mächtig: Algorithmen entscheiden, ob wir einen Job bekommen oder nicht, wie kreditwürdig wir sind, welche Nachrichten wir sehen, was wir lesen, sehen und hören. Für viele Menschen klingt das mittlerweile mehr wie eine Drohung als eine Verheißung. So bedrohlich, dass inzwischen auch die Politik aufgewacht ist: Die Bundesregierung etwa berief eine Datenethikkommission ein.

Im Herbst 2019 legten die 16 von der Bundesregierung eingesetzten Experten ein erstes Gutachten vor. Mit drastischen Forderungen: Unter anderem empfahl die Kommission ein risikoadaptiertes Regulierungssystem für den Einsatz algorithmischer Systeme, eine Bewertung von Programmen nach „Kritikalität“ und „Schädigungspotenzial“ und sogar ein komplettes Verbot der allerschädlichsten Programme.

Ist das eine vernünftige Abwägung der Risiken technischer Entwicklung oder die Angst vor der Allmacht der Maschine? Eine Angst, die sich mehr aus popkulturellen Bildern und überzogenen Marketing-Versprechen speist als aus konkretem Wissen? Dieser Schwerpunkt soll diese Diskussion versachlichen: Er zeigt in den folgenden Artikeln anhand von zehn Beispielen, was Algorithmen so bedeutsam macht und wo ihre Risiken und Nebenwirkungen liegen.

Der Kontext macht den Unterschied

Im Kern sind Algorithmen in der IT zunächst nichts weiter als eine Folge von Rechenanweisungen. Was sie so mächtig und gelegentlich problematisch macht, ist nicht ihre Ausführung, sondern der Kontext, in dem sie entworfen und verwendet werden. Denn um abstrakte Probleme für Computer berechenbar zu machen, muss die Problemstellung auf ein mathematisches Modell abgebildet werden. Der betreffende Algorithmus löst dann dieses mathematisch abstrahierte Problem.

Das Auto kann nicht mehr bremsen, wen soll es überfahren? Derzeit sind solche Überlegungen noch Gedankenspiele. Eines Tages müssen selbstfahrende Autos aber vielleicht genau solche Entscheidungen treffen.Die abstrakte Lösung kann dann auf alle möglichen konkreten Probleme angewandt werden. Einem Sortier-Algorithmus beispielsweise ist es egal, ob er Zahlenwerte sortiert, Produkte nach Beliebtheit oder Bilder nach ihrem Motiv. So gesehen sind Algorithmen wirklich so mächtig, präzise, unbestechlich und objektiv, wie viele Menschen glauben.

Ein kritischer Punkt dabei ist jedoch, wie genau eigentlich unscharfe, subjektive Größen wie Beliebtheit, Schönheit oder auch die Eignung für einen Job in Zahlenwerte übersetzt werden – die sogenannte Objektivierung. Denn das mathematische Modell kann immer nur einen kleinen Ausschnitt aus der Realität abbilden. Welche Größen wie genau mathematisch abgebildet werden, kann jedoch großen Einfluss auf das Ergebnis einer Berechnung haben. Wer unsinnige Daten eingibt, wird unsinnige Ergebnisse bekommen. „Garbage in, garbage out“, wie der Informatiker sagt.

Dazu kommt, dass oftmals nicht alle Daten zur Verfügung stehen, die für eine exakte Berechnung notwendig wären. Ein autonomes Auto beispielsweise muss seine nächsten Aktionen anhand äußerst lückenhafter Sensordaten planen – und noch dazu damit rechnen, dass sich die Situation während der Planung weiter verändert.

Die Antwort der Informatik darauf sind Vereinfachungen, die oft, aber nicht zwingend immer zum Ziel führen: Sie vergleichen – ähnlich, wie es der Mensch tun würde – die Situation mit früheren Erfahrungen, versuchen die Konsequenz einer falschen Entscheidung abzuschätzen, treffen Annahmen über die zukünftige Entwicklung – und im Zweifelsfall lassen sie den Zufall per Münzwurf entscheiden.

Diese Erkenntnis ist alles andere als beruhigend. Denn sie bedeutet, dass die Bewertung und Regulierung von Algorithmen von ihrem Kontext abhängt. Die Annahmen, unter denen Algorithmen zum Einsatz kommen, sind genauso zu hinterfragen wie die Datenbasis und die heuristischen Methoden. An dieser Diskussion wird kein Weg vorbeiführen. Der Artikel ab Seite 36 gibt den aktuellen Stand dieser Diskussion um die „Ethik der Algorithmen“ wieder. (jo@ct.de) c't

Auf dem Weg zum Öko-Akku

Es lässt sich nicht leugnen: Die Herstellung der Batterien belastet die Umweltbilanz von E-Autos erheblich. Es gibt aber bereits reichlich Ansätze, ihren ökologischen Fußabdruck deutlich zu verkleinern.

VON DENIS DILBA, GREGOR HONSEL UND WOLFGANG RICHTER

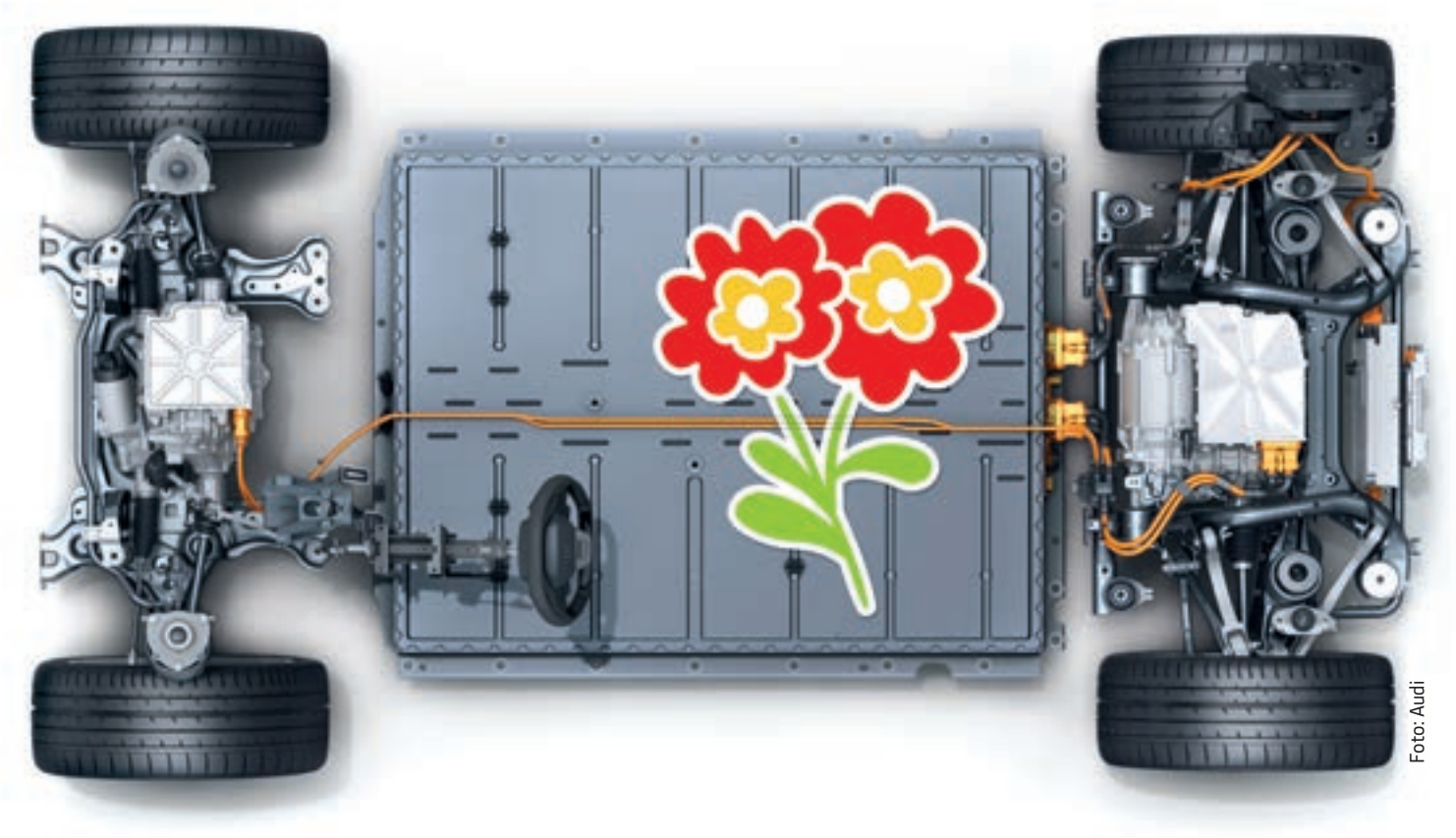


Foto: Audi

Mit der einen Million Elektroautos, die nach dem Plan der Bundesregierung im Jahr 2020 auf deutschen Straßen fahren sollen, wird das nichts mehr. Derzeit sind es gerade einmal 83 000. Doch allein in China wurden 2018 knapp 1,3 Millionen E-Fahrzeuge abgesetzt, in den USA waren es rund 350 000. Das zeigt: Der Markt ist in Bewegung gekommen.

Ist das wirklich eine gute Nachricht für die Umwelt? Kritiker verweisen darauf, dass die Produktion der Batterien gewaltige Ressourcen an Energie und Rohstoffen verschlingt – womöglich mehr, als das Auto während seiner Lebensdauer einspart.

Diese Einwände sind nicht von der Hand zu weisen. Auch wenn die Mehrheit der Studien dem E-Auto unter dem Strich eine bessere Ökobilanz bescheinigt als einem Benziner oder Diesel (siehe Tabelle S. 72): Es gibt noch viel Luft nach oben. Wir haben uns angeschaut, mit welchen Stellschrauben sich die Herstellung der Batterien umwelt- und menschenfreundlicher machen lässt. Einen großen Hebel bieten die Rohstoffe: Sie lassen sich durchaus nachhaltig gewinnen, auch wenn die entsprechende Zertifizierung kompliziert ist. Besonders kritische Materialien wie Kobalt können auch ersetzt oder zumindest stark reduziert werden (Seite 67).

Vor allem um das Thema Energieverbrauch geht es bei der Produktion. Hier haben Forscher bereits viele Möglichkeiten entdeckt, die Prozesse effizienter zu machen (Seite 68). Das gilt auch für das Recycling. Zwar wird es noch ein paar Jahre dauern, bis Akkus in nennenswerten Mengen ausgemustert werden, doch für diesen Zeitpunkt sollte die Industrie vorbereitet sein. Und das sind einige Unternehmen bereits (Seite 70).

(grh@heise.de) c't

Nachhaltig fördern

Material für Batterien wird oft unter fragwürdigen Bedingungen gewonnen. Konzerne schließen sich zusammen, um das zu ändern.

Wer Tobias Tretter zu einer Lithium-Förderstätte begleitet, sollte höhenerprobt sein: Mehr als die Hälfte der weltweiten Lithiumvorkommen lagern in einem bis zu 4000 Meter hohen Plateau in den Anden, das sich Chile, Argentinien und Bolivien teilen – in Salzseen unter offenem Himmel. „Es kommt recht häufig vor, dass einer meiner Begleiter im Jeep auf dem Weg dorthin Symptome der Höhenkrankheit entwickelt“, sagt der Geschäftsführer der Commodity Capital AG – einer sogenannten Fondsboutique, die weltweit in Rohstoffunternehmen investiert. „Wir haben daher immer eine Sauerstoffflasche dabei.“ Er selbst habe Glück und sei wenig anfällig. Selbst nach einem stundenlangen Trip über staubige Pisten ist Tretter oft noch fit genug, die Lagerstätte direkt in Augenschein zu nehmen.

Der Fondsmanager vertraut nur dem, was er selbst gesehen hat. Er trägt Verantwortung für seine Investoren, und da bleibt ihm oft gar nichts anderes übrig: Einen weltweiten Ökostandard oder ein Zertifikat für nachhaltiges Lithium gibt es nicht. Auch bei Kobalt ist ein Gütesiegel erst in den Anfängen.

Dabei ist das Problem drängend. Lithium führt bei seinem Abbau zu Umweltschäden, Kobalt stammt überwiegend aus der diktatorisch geführten „Demokratischen Republik Kongo“, wo oft Kinder im illegalen Kleinbergbau unter oftmals lebensgefährlichen Bedingungen eingesetzt werden, wie ein viel beachteter Report von Amnesty International Anfang 2016 offenlegte. Die Deutsche Rohstoffagentur geht in einer aktuellen Studie davon aus, dass sich das Problem durch den Elektromobilitätsboom verschärfen wird. Aus diesem Grund investiert Commodity Capital nicht in afrikanische Kobaltminen wie im Kongo, denn Nachhaltigkeit liegt im Eigeninteresse der Investoren – je länger die Anlage ohne Probleme läuft, desto länger wird dort Geld verdient.

Immerhin ist seit dem Kobaltreport von Amnesty zumindest etwas Bewegung in die Sache gekommen: Um die Arbeitsbedingungen zu verbessern, haben sich Ende 2016 Unternehmen wie Apple, HP, Huawei, Samsung SDI und Sony zur „Responsible Cobalt Initiative“ zusammengeschlossen. Auch Daimler, BMW und Volkswagen wollen in verschiedenen Partnerschaften und Initiativen die Arbeits- und Lebensbedingungen der Einheimischen verbessern.

Eine besondere Rolle spielt dabei die Zertifizierung der Kobaltschmelzen vor Ort, weil diese einen starken Einfluss auf ihre Zulieferer haben. VW setzt zusätzlich auf die Blockchain, um die Herkunft der Mineralien durch die gesamte Lieferkette zurückverfolgen zu können. „Unternehmen, die Kobalt aus illegalem Kleinbergbau einkaufen, kommen nicht in unsere Lieferkette“, sagt Frank Blome, Leiter des Center of Excellence Batteriezelle bei VW.

Johanna Sydow, Expertin für Ressourcenpolitik bei der Umweltorganisation Germanwatch, begrüßt solche Schritte, mahnt aber an, dass viele Zertifizierungsprogramme kaum Änderungen in den Minen bewirkten. Auch BMW gibt zu: Alle Hersteller seien zwar bemüht, die Lieferkette „sauber zu halten“, ein gewisses Restrisiko bleibe aber bestehen. Zum jetzigen Stand werden die Bayern ihr Kobalt ab 2020 nicht mehr aus dem Kongo beziehen, sondern aus einer australischen Mine des Schweizer Rohstoffriesen Glencore.

Die Unternehmen haben also durchaus Alternativen zu Staaten ohne Umweltauflagen. „In erster Linie sind dies die Länder in Afrika und einigen Teilen Südamerikas“, sagt Tretter. Aber grundsätzlich sei die Minenindustrie oft „grüner“, als man annehmen würde. Insbesondere Bergbaukonzerne aus Kanada und Australien, die sowohl Lithium als auch Kobalt liefern, unterlägen strengen Regularien. „Da gibt es keine Abbaugenehmigung ohne gründliche Überprüfung der ökologischen Verträglichkeit“, sagt Tretter. „Die Konzerne müssen detailliert darlegen, wie sie die Eingriffe in die Natur nach dem Abbau wieder rückgängig machen oder die Altlasten umweltfreundlich entsorgen – und noch vor Produktionsstart die benötigten finanziellen Mittel zurückstellen.“

Tretter sieht das eigentliche Problem daher woanders. Zumindest bei Lithium „wird die entscheidende Frage nicht sein, ob zertifiziert oder nicht – sondern ob man das Material überhaupt noch bekommt“.

Für die angekündigten Elektromodelle brauchen die Hersteller in fünf bis sieben Jahren drei Millionen Tonnen Lithium pro Jahr. Derzeit seien es noch rund 250 000 Tonnen. „Es gibt zwar weltweit genug Rohstoff im Boden – wir bekommen ihn nur leider nicht so schnell gefördert, wie er benötigt wird. Ich befürchte, der eine oder andere Hersteller muss seine Elektromobilitätsziele deutlich nach unten korrigieren.“ DENIS DILBA

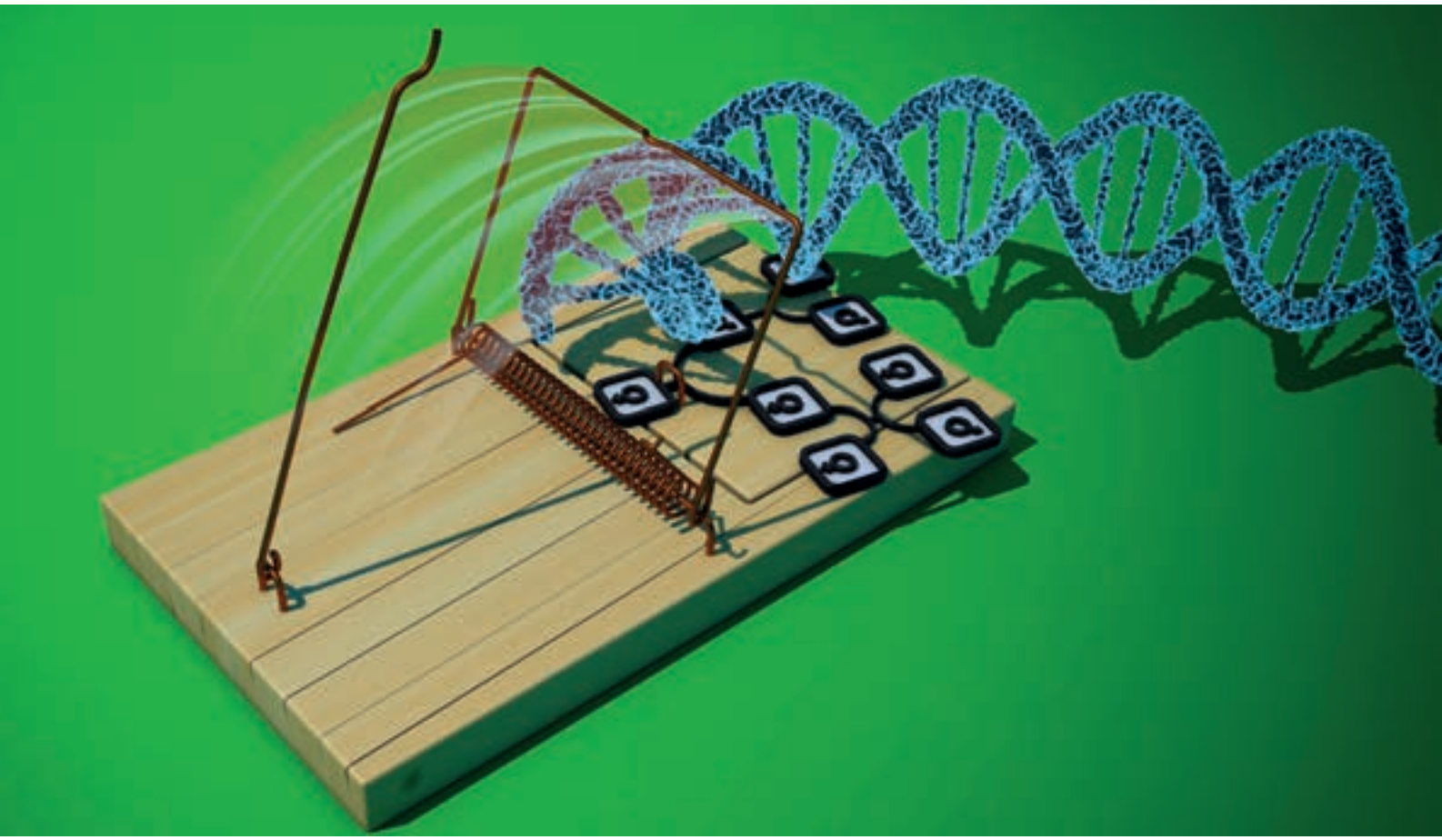
Neue Materialien verwenden

Auf der Suche nach umweltfreundlichen Ausgangsstoffen werden Batterieforscher an überraschenden Stellen fündig.

Was wäre ein wirklich umweltfreundliches Material für eine Batterie? Forscher des Helmholtz-Instituts Ulm probieren es mit matschigen Äpfeln. Sie zerkleinern nicht mehr essbares Obst und geben die Stücke in ein großes Becherglas. „Und zwar mit Kerngehäuse und Stiel, denn im industriellen Maßstab wäre es nicht effizient, diese Teile herauszusieben“, sagt Institutsdirektor Stefano Passerini. Nach einem Tag bei 80 Grad im Trockenschrank sind daraus braune, harte Brocken geworden, welche die Forscher in einem Mörser zerkleinern. Sie wollen an den Kohlenstoff darin herankommen – und daraus die Anode von lithium- und kobaltfreien Akkus herstellen.

Die Anode speichert die positiven Ionen beim Laden. Beim Entladen wandern sie durch einen Elektrolyten zur Kathode. Dabei passieren sie eine Separatorfolie aus Polyethylen, die zwar Ionen durchlässt, Elektronen aber nicht. Diese müssen sich über einen äußeren Stromkreis bewegen und treiben dabei zum Beispiel einen Elektromotor an (siehe Grafik S. 68).

Statt Lithium- können auch Natrium-Ionen als Ladungsträger dienen. Natrium ist eines der häufigsten Elemente auf der Erde und entsprechend preiswert. Das übliche Graphit als Anodenmaterial funktioniert dann allerdings nicht mehr, weil die Natrium-Ionen größer sind. Hier braucht es amorphen Kohlenstoff – wie den aus den Apfelresten. Laut Helmholtz-Institut lässt sich dieses Material deutlich günstiger aus Bioabfall statt aus fossiler Kohle gewinnen. Zudem entstehen so weniger Treibhausgase, als wenn die Bioreste vergären würden. Weiteres CO_2 ließe sich einsparen, wenn der Kohlenstoff auch aus Zucker-



Datensammler entdecken die DNA ihrer Kunden als Kapital

Eine DNA-Analyse ist leicht bestellt und kostet nur kleines Geld. Die Ergebnisse aus US-Laboren sollen dem Kunden mehr über sich selbst verraten – sie dienen aber zugleich der Forschung, der Pharmaindustrie und Ermittlungsbehörden.

VON ARNE GRÄVEMEYER

So verlockend preisgünstig sind DNA-Analysen noch nie gewesen. 59 Euro kostet aktuell ein einfacher Test auf den konkurrierenden Ahnenforschungsplattformen Ancestry.de und MyHeritage.de. Mit den Analyseergebnissen versprechen die Anbieter eine Herkunftsanalyse und sogar die Identifizierung von Blutsverwandten. Das ist möglich, da sie in den vergangenen Jahren große Bestände an DNA-Rohdaten gesammelt haben.

Ancestry wirbt beispielsweise mit über 15 Millionen Kunden. Das Unternehmen startete seine DNA-Tests bereits 2012 in den USA und weitete das Angebot bis 2016 international aus. Eine umfangreiche Datenbank verspricht eine hohe Trefferzahl bei der Suche nach Verwandten. Derzeit lebt der größte Teil der Ancestry-Kunden in Nordamerika, wodurch regelmäßig auch für deutsche Nutzer überproportional viele entfernte Verwandte aus dieser Region gefunden werden.

MyHeritage verwaltet nach eigener Aussage einen Pool von immerhin 3,8 Millionen Kunden, eingesammelt seit der Einführung der DNA-Analysen im November 2016. Auch MyHeritage findet seine Kunden überwiegend in Nordamerika, bezeichnet sich aber mit über 2,1 Millionen Nutzern allein in Deutschland als Marktführer in Europa. Es ist allerdings schwierig einzuschätzen, wie viele DNA-Analysen aus Europa mittlerweile bei MyHeritage gespeichert sind. Die meisten der genannten Nutzer pflegen zunächst nur die Daten ihres Familienstammbaums auf der Online-Plattform und tauschen darüber Familienneuigkeiten mit Angehörigen aus.

DNA auf unbestimmte Zeit eingelagert

Wer sich bei der Bestellung eines DNA-Testkits in die Datenschutzvereinbarungen vertieft, der erkennt, dass er mit der Abgabe seiner DNA-Probe auch weitreichende Rechte abtritt (siehe auch S. 88). So kündigen sowohl Ancestry als auch MyHeritage an, die DNA-Probe nach der Laboranalyse nicht etwa zu zerstören, sondern dauerhaft zu lagern. Mit der Übermittlung der Probe gibt der Kunde beispielsweise MyHeritage die Erlaubnis, „genetische Analysen mit heute verfügbaren DNA-Methoden und solchen, die in der Zukunft entwickelt werden, auszuführen". Nochmalige DNA-Analysen in der Zukunft werden explizit nicht ausgeschlossen. Das ist nicht nur nachteilig, denn spätere Tests lassen umfangreichere Ergebnisse erwarten. Der Kunde gibt aber die Kontrolle aus der Hand.

Darüber hinaus leitet das Unternehmen die Analyseergebnisse an Forschungseinrichtungen weiter. Auf der anderen Seite räumt es dem Kunden „keine Rechte an der Forschung oder irgendwelchen kommerziellen Produkten ein", die noch entwickelt werden könnten und sich auf seine DNA beziehen. Wenigstens kann der Kunde nachträglich die Vernichtung seiner DNA-Probe verlangen. Er ist auch nicht gezwungen, seine Analyseergebnisse für die Forschung freizugeben.

Ganz ähnlich regelt Ancestry den Datenschutz. Die abgegebene Speichelprobe wird bis auf Weiteres für künftige Analysen gelagert. Auch Ancestry stellt DNA-Analyseergebnisse einzelnen Forschungsprojekten zur Verfügung und bittet dafür um die Einwilligung des Nutzers. Das Unternehmen nutzt die DNA selbst für wesentlich mehr als nur zur Suche von Verwandtschaftsbeziehungen: „Ihre DNA-Daten werden auch verwendet, um andere Angaben über Sie zu erstellen, wie ... Haardicke und Augenfarbe oder Merkmale, die mit Ihrer Gesundheit und Ihrem Wohlbefinden verbunden sind." Und wer sich etwa per Facebook anmeldet, dessen öffentliche Profilinformationen sammelt Ancestry ebenfalls ein (laut Datenschutzerklärung vom 25. Juli 2019).

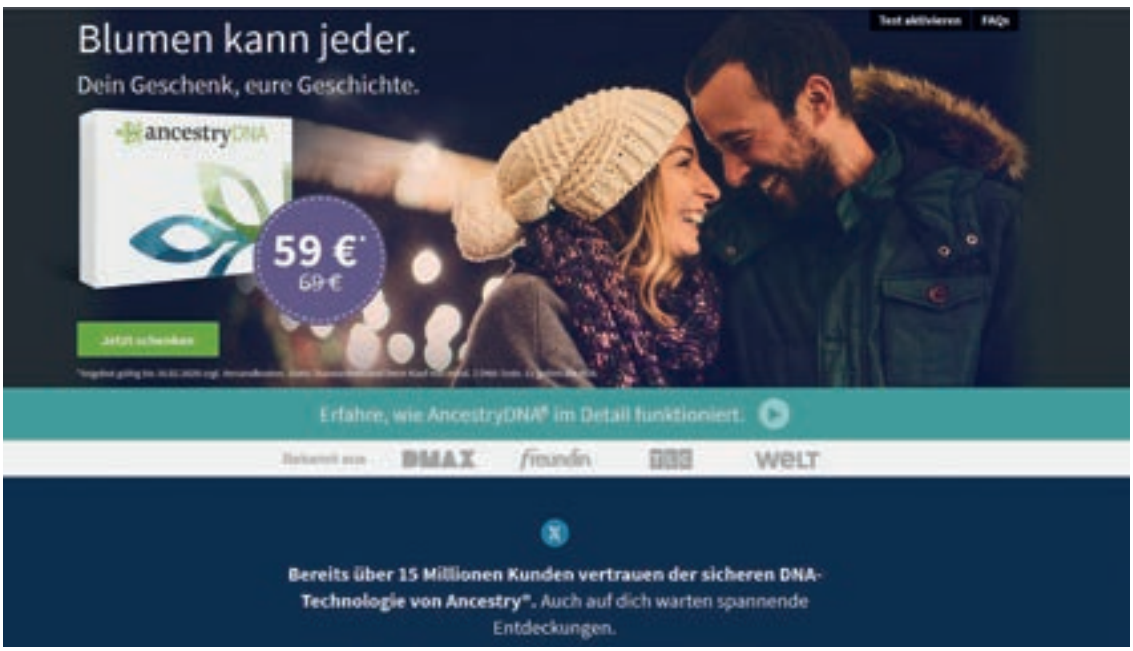
Künftig Probleme mit Versicherern?

Redakteure der c't haben die DNA-Analyse bei MyHeritage und bei Ancestry ausprobiert, allerdings unter falschen Namen (siehe S. 92). Dass in der DNA des Menschen viel mehr Potenzial steckt als nur etwas Unterstützung beim Aufbau eines Familienstammbaums, wird dem Besteller klar, wenn er die „Patienteninformation und Einwilligungserklärung" von Ancestry liest. Zu den Risiken gehört nämlich nicht nur, dass der Kunde unerwartete Verwandtschaftsverhältnisse entdeckt und so seinen Familienfrieden gefährdet. Es bestehe auch ein Risiko, dass die Analysedaten aufgrund eines Fehlers an die Öffentlichkeit gelangen. „Dies könnte negative Auswirkungen darauf haben, einen bestimmten Versicherungsschutz zu erlangen, oder Ihre Daten könnten von Strafverfolgungsbehörden verwendet werden, um Sie zu identifizieren."

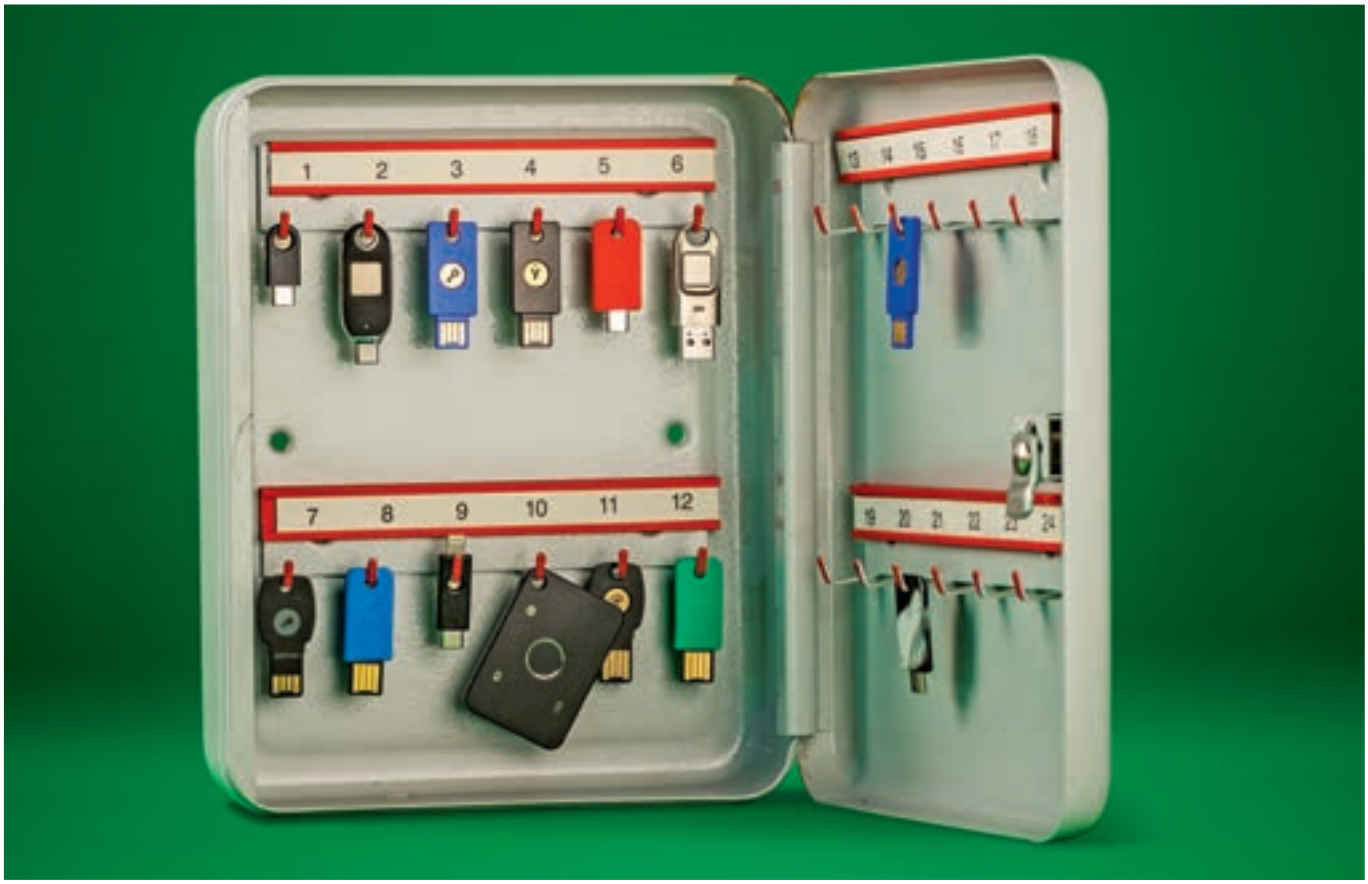
Versicherer dürfte das Feld der Erbkrankheiten interessieren, auf dem Forscher regelmäßig neue Zusammenhänge entdecken. Dass ein erhöhtes Risiko für schwerwiegende Erkrankungen den Versicherungsschutz verteuern könnte, kann man sich leicht ausmalen. Und das gilt im Zweifel nicht nur für den Einzelnen, sondern auch für seine Eltern, seine Kinder und Kindeskinder. Die Gefährdung durch eine DNA-Analyse heute ist damit für die Zukunft gar nicht abzuschätzen.

Das Potenzial der DNA-Datenbanken für Strafermittler belegte der Fall des sogenannten Golden-State-Killers im Jahr 2018. Um einen Serienmörder nach über 30 Jahren zu überführen, nutzten die Beamten DNA-Spuren vom Tatort, legten Profile bei Ahnenforschungsplattformen an und fanden in deren Datenbanken ähnliche Erbgutprofile. Im familiären Umfeld der zugehörigen Kunden entdeckten die Ermittler schließlich den später Verurteilten.

Seit November 2019 erlaubt ein Erlass des US-Justizministeriums dieses



So billig wie noch nie: Als Aktionspreis locken Ahnenforschungsplattformen mit DNA-Analysen schon für 59 Euro.



FIDO2-Sticks zum Einloggen

mit und ohne Passwort

Mit einem Sicherheitsschlüssel schützen Sie Ihre Accounts effektiv vor Phishing und Trojanern. Spielt der Dienst mit, können Sie sich sogar ohne Benutzername und Passwort einloggen. Manche Sticks eignen sich auch zur Mail-Verschlüsselung. Wir haben die derzeit erhältlichen Modelle ausprobiert, um Ihnen den Kauf zu erleichtern.

VON RONALD EIKENBERG

Das Login-Verfahren FIDO2 ist die Lösung für viele Probleme: Es schützt Ihre Online-Accounts vor Phishing, Trojanern und Passwortklau. Dabei dient es entweder als zweiter Faktor zusätzlich zum Kennwort – oder sogar als Passwortersatz. Wenn der Dienst die technischen Möglichkeiten der neuen Technik ausreizt, dann können Sie sich die lästige Eingabe Ihres Benutzernamens und Ihres Passworts schenken. Wie komfortabel das sein kann, können Sie bereits bei den Microsoft-Diensten ausprobieren. Anfänglich klappte das nur mit dem Edge-Browser, inzwischen hat Microsoft das Einloggen ohne Passwort aber auch für andere Browser unter Windows 10 freigegeben.

Das FIDO2-Verfahren ist nicht nur sehr bequem, sondern auch sehr sicher. Sie authentifizieren sich mit einem sogenannten Sicherheitsschlüssel (oder auch Authenticator, zu Deutsch: Authentifikator) bei den Diensten. Zum Einloggen reicht oft ein Knopfdruck. Ist mehr Sicherheit gefragt, dann wird der FIDO-Schlüssel mit einer PIN entsperrt. So ist gewährleistet, dass eine unbefugte Person, der Ihr Schlüssel in die Hände fällt, sich nicht einfach in Ihre Accounts einloggen kann. Das Prinzip ist vergleichbar mit einer EC-Karte: Da nur wenige Fehlversuche erlaubt sind, reicht eine vierstellige PIN aus. Bei FIDO2 sind auch längere, alphanumerische PINs erlaubt. Eingeben muss man sie etwa dann, wenn ein Dienst komplett auf die Eingabe von Benutzername und Passwort verzichtet. Noch bequemer wird es, wenn man die PIN-Eingabe durch Biometrie ersetzt

und den Sicherheitsschlüssel einfach per Fingerabdruck entsperrt. Die Überprüfung erfolgt in jedem Fall lokal – der Dienst erfährt, dass Sie sich verifiziert haben und somit vertrauenswürdig sind, es wird jedoch niemals PIN oder Fingerabdruck übertragen. Die Technik hinter FIDO2 haben wir ausführlich in c't 18/2019 vorgestellt.

Dieses Mal geht es um die Sicherheitsschlüssel, die es bereits in allen Farben und Formen gibt. Am meisten verbreitet ist das USB-Stick-Format. Die einfachsten Ausführungen kosten rund 20 Euro und haben einen Knopf, über den man den FIDO2-Vorgang bestätigt. Ist eine PIN nötig, wird sie auf dem Rechner abgefragt. Wer ein paar Euro mehr ausgibt, bekommt Exemplare mit Fingerabdruckscanner, welche die PIN-Eingabe obsolet machen. Bei den Anschlüssen ist fast alles vertreten, was derzeit möglich ist: Es gibt Sicherheitsschlüssel mit USB-A, USB-C, Lightning, Bluetooth und NFC. Man hat aktuell im Wesentlichen die Wahl zwischen drei Herstellern: Feitian, SoloKeys und Yubico. Jeder davon bietet etliche Modelle an – mit unterschiedlichen Anschlusskombinationen und oft auch unterschiedlichen Funktionen. Wir haben fast alle FIDO2-Sicherheitsschlüssel bestellt, die derzeit erhältlich sind, und ausführlich getestet.

Das wichtigste Kriterium bei der Auswahl der Produkte war Zukunftssicherheit. Denn nicht alle Sicherheitsschlüssel beherrschen etwa das Einloggen ohne Benutzername und Passwort, das in Zukunft nicht länger nur Microsoft anbieten wird, sondern hoffentlich viele weitere Dienste. Dazu muss der Authenticator in der Lage sein, bei der Registrierung den für den Dienst generierten Krypto-Schlüssel zu speichern, den sogenannten Resident Key. Kann der Authenticator das nicht, wird der Krypto-Key verschlüsselt beim Anbieter abgelegt. Dann muss der Authenticator den Key bei jeder Anmeldung zunächst beim Dienst abholen, wozu der Anwender mindestens seinen Benutzernamen eintippen muss – anders kann der Dienst nicht den richtigen Key heraussuchen.

Eine weitere wichtige Funktion ist die User Verification. Ein Dienst kann verlangen, dass sich der Nutzer durch PIN, Fingerabdruck oder Gesichtsscan gegenüber dem Authentifikator verifiziert. Und zwar auch dann, wenn keine Resident Keys zum Einsatz kommen. Wer auf der sicheren Seite sein will, sollte also zu einem Sicherheitsschlüssel greifen, der sowohl Resident Keys speichern kann als auch die User Verification beherrscht. Insbesondere alte Authentifikatoren können weder das eine noch das andere. Sind sind nur „FIDO U2F"-zertifiziert (auch FIDO1 genannt) und außen vor, sobald ein Dienst von den mit FIDO2 eingeführten Funktionen Gebrauch macht. U2F-Authentifikatoren sind derzeit noch massenhaft im Verkauf, Sie sollten beim Kauf also genau hinsehen.

Der FIDO2-Vorgänger U2F ist als zweiter Faktor konzipiert, das Einloggen ohne Passwort klappt damit nicht. Da der Standard älter als FIDO2 ist, unterstützen ihn mehr Dienste. Wer möglichst viele Accounts per Sicherheitsschlüssel absichern will, kommt daher derzeit nicht an U2F vorbei. Es nutzt eine andere Browser-Schnittstelle als FIDO2, welche Authenticator und Browser unterstützen müssen. Die gute Nachricht ist, dass fast alle FIDO2-Sicherheitsschlüssel auch U2F beherrschen. Das unterscheidet sie übrigens von den internen Sicherheitsschlüsseln von Windows 10, Android und macOS (siehe c't 18/2019, S. 20).

Viele Sicherheitsschlüssel belassen es nicht dabei, ihren flexiblen Security-Chip für FIDO2 und U2F zu nutzen. Die YubiKeys von Yubico bieten allerlei Zusatzfunktionen, die mit Authentifizierung und Verschlüsselung zu tun haben, etwa die Erzeugung von Einmalpasswörtern nach dem OTP-Verfahren oder den Einsatz als OpenPGP-Smartcard. Mehr zur Nutzung der OTP-Funktion finden Sie ab Seite 112, den Einsatz als OpenPGP-Smartcard beschreiben wir ab Seite 116. Besonders zukunftssicher sind die Solo-Authenticators von SoloKeys: Ihre Firmware steht nicht nur unter einer Open-Source-Lizenz, sie lässt sich auch nachträglich aktualisieren. Auf diese Weise kann der Hersteller neue Funktionen nachliefern. Feitian hat als einziger Hersteller Sicherheitsschlüssel mit Bluetooth und Fingerabdruckscanner im Sortiment. Hier sind die Unterschiede innerhalb der Produktpalette am größten. Wir stießen auf viel Licht, aber auch auf viel Schatten.

SoloKey

Die Solo-Familie von SoloKeys setzt voll und ganz auf Open Source: Sowohl

Benutzername und Passwort? Nicht nötig. Wer einen FIDO2-Stick im Einsatz hat, klickt einfach auf „Mit Windows Hello oder einem Sicherheitsschlüssel anmelden".

Simple FIDO2-Authentifikatoren wie den Security Key von Yubico bekommt man schon für 20 Euro.

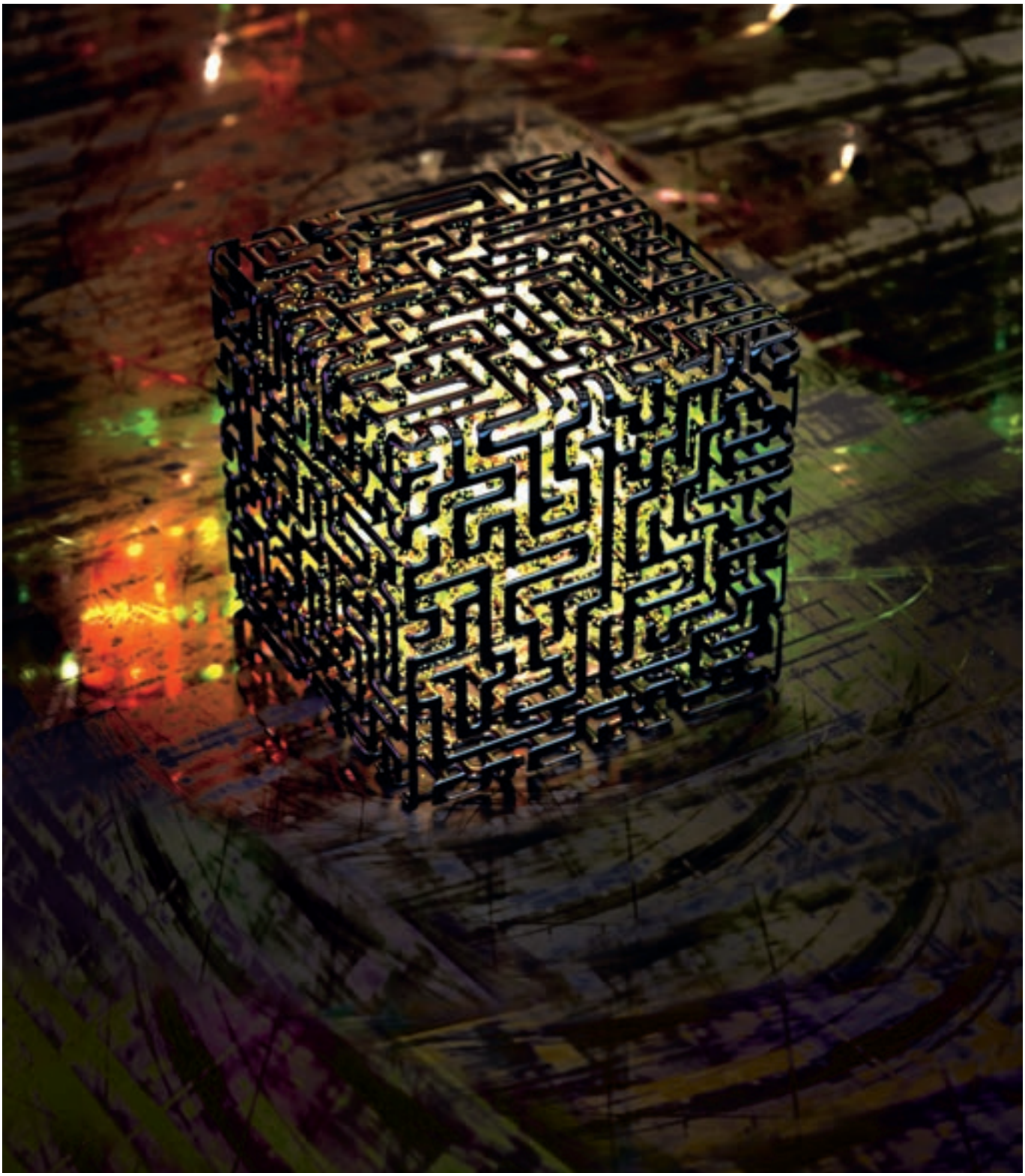


Foto: Shutterstock

Blick in die Wunderkiste

Quantencomputer können viele Rechenoperationen parallel abarbeiten – dank der besonderen Spielregeln der Quantenwelt. Welche Hardware sich dafür am besten eignet, ist noch offen. Vor allem drei Typen sind im Rennen.

VON NIELS BOEING, ALEXANDER BRAUN, WOLFGANG RICHTER UND WOLFGANG STIELER

Im Zeitalter der Hochtechnologien ist ein Bonmot von Arthur C. Clarke zur Alltagsweisheit geworden, die in keiner Trendbroschüre fehlen darf. „Jede hinreichend fortgeschrittene Technologie ist von Magie nicht mehr zu unterscheiden“, schrieb Clarke 1973 in „Profiles of the Future“. Inzwischen scheinen sich auch IT-Konzerne damit abzufinden, wenn etwa IBM Quantencomputer in populärwissenschaftlichen Grafiken mit der „Magie der Quantenalgorithmen“ erklärt.

Der Grund dafür liegt in einer prinzipiellen Erkenntnis der Quantenmechanik aus den 1920er-Jahren: Ein physikalisches System des Quantenkosmos ist nicht in einem einzigen festgelegten Zustand, sondern in einer Überlagerung verschiedener möglicher Zustände. Während ein Bit dadurch dargestellt wird, dass am Ausgang eines Schaltkreises Strom fließt oder nicht (1 oder 0), lässt sich ein Qubit durch unterschiedliche Quantensysteme abbilden, die zwei Werte gleichzeitig annehmen können. Während ein zweistelliges Register aus zwei klassischen Bits eine einzige Zahl darstellen kann, kann ein zweistelliges Register aus zwei Qubits vier Zahlen darstellen. Ein zehnstelliges Register aus Qubits steht dann parallel für 1024 Zahlen.

Was genau sind diese „überlagerten Quantenzustände“, und wie kann man damit rechnen? Um das zu verstehen, muss man das Konzept der Wahrscheinlichkeitswellen erklären. Auf ihm beruhen alle Quantenrechner. Das gelingt am besten mit einem Experiment, das 2002 in einer Umfrage des britischen Institute of Physics zum „schönsten Experiment aller Zeiten“ gewählt wurde.

Stellen Sie sich vor, man schießt Elektronen auf eine Wand mit zwei nebeneinanderliegenden Schlitzen. Elektronenstrahlen haben genauso wie Lichtstrahlen Welleneigenschaften. Hinter jedem Schlitz bilden sich daher kreisrunde Wellen, die wie Wasserwellen ineinanderlaufen und sich dabei gegenseitig mal abschwächen, an anderer Stelle aber verstärken. Dieser Interferenz genannte Vorgang erzeugt auf einer dahinterliegenden Wand, in der die Elektronen einschlagen, schließlich ein charakteristisches Streifenmuster.

Jedoch, und das ist das Kuriose, bildet sich dieses Muster auch, wenn man die Elektronen einzeln nacheinander auf die beiden Schlitze schießt. Eine einzelne „Elektronenwelle“ muss also durch beide Schlitze gleichzeitig gehen – sonst kann es keine Abschwächung und Verstärkung geben. Wie kann das sein? Das Elektron kann sich schließlich nicht aufgeteilt haben. Also kamen die Physiker mit dem Konzept der Wahrscheinlichkeitswellen um die Ecke. Ob es die nun wirklich gibt oder sie nur ein mathematisches Konstrukt sind, darüber streiten sich noch die Philosophen.

Auf jeden Fall schreibt die Quantenphysik jedem Quantenobjekt eine Welle zu, deren Betrag die Wahrscheinlichkeit angibt, das Objekt anzutreffen. Die Frage, an welchem Ort mit welcher Wahrscheinlichkeit ein Elektron gemessen werden kann, ist aber nur ein Spezialfall. Verallgemeinert ist ein Quantenzustand die Beschreibung eines Quantensystems in Bezug auf eine physikalische Größe. Man kann sich das wie ein Koordinatensystem vorstellen. Je nachdem, wie das Koordinatensystem gewählt wird, fällt die Beschreibung aus, auch wenn es immer um denselben Punkt im Raum geht.

Qubits, also die Informationseinheiten, mit denen Quantencomputer rechnen, lassen sich durch zwei Basiszustände beschreiben: Bei einem Elektron kann der Spin – oft lax als Eigendrehimpuls bezeichnet – nach oben oder nach unten zeigen. In supraleitenden Schleifen kann Strom bei ultrakalten Temperaturen widerstandslos mit oder gegen den Uhrzeigersinn kreisen. In Ionen können sich Elektronen im Grundzustand oder in einem angeregten Zustand befinden.

Was aber machen die Forscher genau, wenn sie einen Quantenalgorithmus auf Qubits anwenden? Als Beispiel sollen Qubits aus den bereits erwähnten supraleitenden Schleifen dienen. Die Umsetzung eines Algorithmus in mehreren Teilschritten lässt sich nun auf drei Ebenen betrachten: auf einer mathematischen, einer schaltungslogischen und einer physikalischen Ebene.

Mathematisch gesehen kann man ein Qubit als Punkt in einem abstrakten Raum mit zwei Basisdimensionen darstellen. Allerdings sind das in diesem Fall komplexe Zahlen. Das Qubit stellt also einen Vektor dar, dessen Spitze an einer Kugel mit dem Radius 1 liegt – der sogenannten Blochkugel. Die verschiedenen Rechenschritte des Algorithmus drehen nun den Vektor von einem einzelnen oder auch mehreren Qubits hin und her. Jeder Rechenschritt entspricht dabei einer „unitären Transformation“, wie Mathematiker sagen. Auf dieser Ebene ist der Algorithmus eine Folge quantenmechanischer Berechnungen mit Matrizen aus komplexen Zahlen.

Etwas weniger abstrakt kann man Rechenschritte auch als Abfolge logischer Verknüpfungen darstellen. Ein „logisches Gatter“ liefert bei bestimmten Eingangswerten einen definierten Ausgangswert. In der klassischen Computertechnik sind Gatter Schaltkreise, die den Input – hineinfließende Ströme – durch eine Reihe von Transistoren leiten. Ein Beispiel ist das Nicht-Gatter: Es kehrt den Bitwert um. Fließt Strom hinein, also eine „1“, fließt keiner heraus, „0“, und umgekehrt. Für Quantencomputer sind analog verschiedene Standardgatter entwickelt worden, die nur auf ein einzelnes oder auch auf zwei oder drei Qubits wirken. Das wichtigste davon, das Hadamard-Gatter, erzeugt die gewünschte Überlagerung zweier Bitzustände in einem Qubit.

Um den Wert der Qubits am Schluss der Berechnung zu messen, muss man prüfen, in welchem der beiden Basiszustände sich jedes einzelne Qubit befindet. Da sich die Qubits in einem überlagerten Zustand befinden, ist das Resultat einer einzelnen Messung jedoch komplett zufällig. Man muss die Rechnung also sehr oft hintereinander ausführen, jedes Mal messen und bekommt so die statistische Verteilung der Basiszustände in den Qubits.

Theoretisch kann man mit einem Quantencomputer arbeiten wie mit einem teuren, komplizierten Analogcomputer. Man „präpariert“ die Qubits in Zuständen, die einem klassischen Input-String entsprechen, wendet Quantengatter an und liest am Schluss das Ergebnis aus. Die Vorteile eines Quantencomputers ergeben sich jedoch für Probleme, bei denen man ausnutzen kann, dass ein Qubit-Register sehr viele Zahlen gleichzeitig repräsentieren kann.

Den ersten Quantenalgorithmus präsentierte der Mathematiker Peter Shor 1994. Eines von zwei Beispielen, die Shor in seinem Paper präsentierte, ist die Zerlegung von Zahlen in Primfaktoren. Nehmen wir die 15: Ihre Primfaktoren sind 3 und 5. Nun kann man die 15 noch im Kopf zerlegen. Bei

Wie man **Campusnetze** plant

Erstmals können Fabriken oder Institute ihre WLAN-gestützten Infrastrukturen mit einem lokalen Mobilfunknetz ergänzen und so ihre Produktion optimieren. Doch wann braucht man ein solches Campusnetz und wie konzipiert man es?

VON TORSTEN MUSIOL UND DUŠAN ŽIVADINOVIĆ

Die Bundesnetzagentur hat aufgrund von Nachfragen aus der Wirtschaft das Funkband zwischen 3,7 und 3,8 GHz speziell für Campusnetze reserviert. Für dieses Band eignen sich bisher nicht viele Geräte, weil es weltweit noch selten in Gebrauch ist. Aber die wichtigsten Produkte gibt es bereits – es handelt sich um Basisstationen, Router, Modems, USB-Sticks und dergleichen, die per LTE kommunizieren. Zuletzt haben die Chip-Hersteller die Entwicklung und Produktion intensiviert. Manche beliefern nicht nur den freien Markt, sondern fertigen auch Chips für Prototypen im Rahmen von Projektgeschäften. Dazu zählt etwa der Chiphersteller Qualcomm, der unter anderem mit Siemens Produkte für Campusnetze entwickelt.

Die 5G-Entwicklung steht zwar noch am Anfang und die Konzepte sind dem heutigen LTE in mancher Hinsicht überlegen, doch man kann ein Campusnetz schon mal auf 4G-Basis aufbauen und bei Verfügbarkeit von 5G-Implementierungen aufrüsten.

Die Bundesnetzagentur teilt die Campusnetzfrequenzen grundsätzlich technologie- und diensteneutral zu. Das bisher für den Campus reservierte Frequenzband eignet sich sowohl für LTE als auch für 5G. Für LTE hat die ITU das Band 43 (3700 MHz bis 3800 MHz) definiert, für 5G das Band n78 (3300 MHz bis 3800 MHz). Daher ist es durchaus möglich, zunächst mit einem oder mehreren 10 MHz breiten Frequenzblöcken und heute verfügbarer LTE-Technik zu starten und später, wenn erforderlich, weitere Frequenzblöcke zu beantragen und 5G-Technik zu ergänzen.

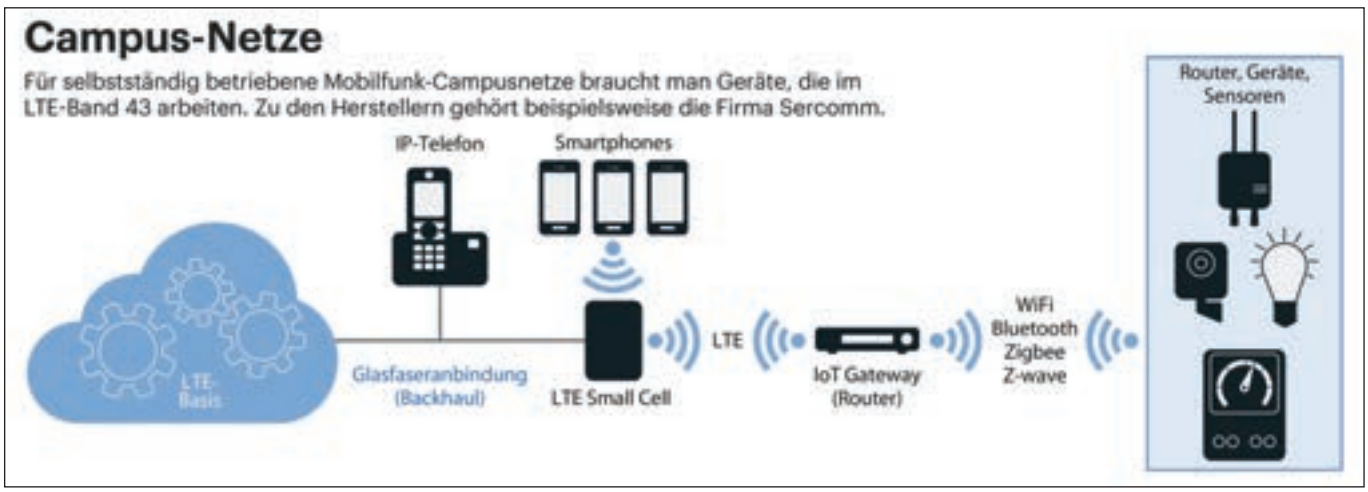
Die Bedingungen wie auch die Kosten für die Zuteilung sind in einer Verwaltungsvorschrift spezifiziert. Bisher ist darin nur Band 43 berücksichtigt. Die Kosten belaufen sich für eine Grundstücksfläche von 500 x 200 Metern (0,1km²), eine Bandbreite von 60 MHz (3 Basisstationen mit je 20 MHz) bei einer Zuteilungsdauer von 10 Jahren auf 2800 Euro oder jährlich 280 Euro. Dasselbe zahlt ein landwirtschaftlicher Betrieb mit 60 Hektar Nutzfläche.

Campusnetze sind hauptsächlich für Unternehmen nützlich, die mit WLAN heute schon an Grenzen stoßen. Wer bereits eine Lizenz für den Campusnetzbetrieb erhalten hat, kann also loslegen. Die Frequenzen im 3,7-GHz-Band sind zunächst für zehn Jahre freigegeben. Vor Ablauf der Frist wird die Behörde den Bedarf erneut prüfen. Für den Fall, dass es keinen Nachschlag gibt, fährt man also besser, wenn man die Anschaffungen möglichst vom ersten Tag an nutzt.

Unter eigener Kontrolle

Die grundsätzliche Strategie wird für viele Unternehmen und Institute ähnlich aussehen: Viele nutzen bereits WLAN zur drahtlosen Vernetzung. Sie werden nicht WLAN-Access-Points einfach so gegen Mobilfunkelemente austauschen, bloß damit alles per Mobilfunk läuft. Das wäre unwirtschaftlich, zumal WLAN für viele Anwendungen ausreicht und die Geräte preisgünstig und ausgereift sind.

Allerdings kann WLAN mit modernem Mobilfunk in vielen Punkten nicht mithalten. Ein nahtloser, umgehender Zellenwechsel (seamless Handover) ist nicht möglich und die Zu-



verlässigkeit und Skalierbarkeit sowie die Möglichkeiten beim Verkehrsmanagement sind weit schlechter. Die Ursache liegt in der zufallsgesteuerten Ressourcenzuteilung, die sich bis hin zur IEEE-Spezifikation 802.11ac durchzieht. So kann man mittels WLAN grundsätzlich keine harten Paketzustellungsfristen festlegen, auch keine festen Geschwindigkeiten. Und aufgrund des zufallsgesteuerten Zugriffs auf das Funkmedium lässt die Effizienz der WLAN-Technik umso stärker nach, je mehr Nutzer eine Basisstation versorgen soll.

Das alles macht schon LTE besser, weil man klar festlegen kann, welches Gerät welche und wie viele Ressourcen erhält. So lassen sich feste Latenzen und feste Geschwindigkeiten garantieren. Das sind Eigenschaften, die in der Industrie generell stark nachgefragt sind. Mit 5G lassen sich allerdings sehr viel mehr Geräte pro Fläche versorgen (siehe Kasten „5G-Spezialitäten“).

So bietet es sich für Industrie und Institute an, ihre WLAN-Netze mit 4G-Technik zu kombinieren und später eventuell mit 5G-Technik zu erweitern. Robuste Anwendungen können hingegen weiterhin das preisgünstige WLAN nutzen; die Prozesse sind ja eingespielt und es gibt keinen Grund, auf Mobilfunk zu wechseln, wenn sie per WLAN zur Zufriedenheit funktionieren. Allerdings bettet man kritische Anwendungen, bei denen WLAN an Grenzen stößt, auf 4G oder 5G um (z. B. für fahrerlose Transportfahrzeuge). Oder man entwickelt sie überhaupt erst, weil sie vorher mit WLAN nicht umzusetzen waren.

Zwei Wege zum Campusnetz

Eine Firma, die ihr WLAN mit einem Campusnetz ergänzt, kann generell zwischen zwei Wegen wählen: Sie kann es in Eigenregie aufsetzen oder einen Netzbetreiber wie Telekom oder Vodafone beauftragen. Dann schnürt der Netzbetreiber ein Angebot, in dem er zum Beispiel festlegt, welche Hard- und Software er für das Kernnetz auf dem Campus, und welchen der Frequenzbereiche, die ihm zur Verfügung stehen, er für das Campusnetz einsetzt. Dabei handelt es sich um Frequenzen, die er im Rahmen von Auktionen ersteigert hat – es sei denn, der Kunde bringt Frequenzen aus dem Band 43 mit. In bisherigen Beispielen zwacken Netzbetreiber aber von den ersteigerten Frequenzen Ressourcen per Network Slicing ab (z. B. Vodafone für den Autohersteller e.Go). Vorteilhaft daran kann sein, dass je nach Funkband das Angebot an Geräten größer ist gegenüber dem aktuellen Angebot für das Band 43 (3,7 bis 3,8 GHz).

Per Network Slicing kann der Betreiber zum Beispiel die für die Firma erforderlichen festen Latenzen einhalten und Verkehrsmanagementkonzepte der Firma umsetzen, also zum Beispiel bedarfsweise die Paketzustellung bestimmter Gerätegruppen bremsen (z. B. Push-To-Talk von Mitarbeitern) oder beschleunigen (Positionsmeldungen von autonomen Fahrzeugen, Robotersteuerung). Jedoch kann der Kunde nicht bestimmen, wie breit das Funkband ist, das der Betreiber zur Abdeckung seiner Firma benutzt, und auch nicht das Frequenzband auswählen — in der Regel muss er nehmen, was ihm der Netzbetreiber anbietet.

Betreibt man ein Campusnetz in Eigenregie, kann man alle Parameter des Campusnetzes selbst kontrollieren: die Frequenznutzung, das User-Management, die Dienste, das User-Equipment und das Verkehrsmanagement. Allerdings braucht man dann auch eigene Support-Mitarbeiter, die es durchgehend am Laufen halten.

Wie findet eine Firma heraus, ob ihr eine Funkvernetzung überhaupt helfen kann?

Dazu orientiert man sich am besten an WLAN. Welche Prozesse hängen aktuell von WLAN ab, welche davon kommen durch die WLAN-Eigenschaften an ihre Grenzen? Ein Autohersteller versorgt zum Beispiel seine Fahrzeuge in der Fertigungsstraße per WLAN mit der benötigten Software. Dabei müssen diverse Betriebssysteme oder auch Navigationskarten in die Autos übertragen werden. Entstehen dabei Wartezeiten bei der Software-Betankung? Wie lang sind sie? Bremsen sie andere Produktionsschritte nennenswert?

Wenn auf mehrere Fragen die Antwort Ja lautet, kann ein Campusnetz Abhilfe bringen. Wenn klar ist, dass sich ein Campusnetz technisch lohnt, muss jede Firma individuell kalkulieren, ob sich die Investition für sie auch rechnet. Wenn zum Beispiel die WLAN-Betankung als Bremspunkt in der Produktion identifiziert worden ist, und das Campusnetz zum Beispiel in Feldversuchen deutlich besseren Durchsatz zeigt, dürfte es sich für einen Autohersteller lohnen, der mehr Fahrzeuge in der gleichen Zeit vom Band rollen lassen will. Aber auch Sicher-

5G-Spezialitäten

5G ist bekannt für kurze Latenzen (geplant: bis zu 1 ms hinunter), hohe Skalierbarkeit (bis zu 1 Million Geräte pro km²) und hohe Datenraten (bis zu 10 GBit/s). Aber diese drei Eigenschaften kann die Technik nicht gleichzeitig liefern. Allerdings braucht man sie auch nicht alle drei auf einmal. Wenn etwa eine Firma in ihrer Fertigung Roboter drahtlos steuern will, dann konfektioniert der Betreiber das Funknetz so, dass es kurze Latenzen erreicht — etwa, damit Stoppsignale des Servers umgehend ausgeführt werden, wenn Menschen einen Gefahrenbereich betreten. In diesem Fall braucht man keine hohe Skalierbarkeit.

Aber beispielsweise kann die Skalierbarkeit für Stadtwerke interessant sein, die viele Stromzähler per 5G auslesen wollen. Dafür brauchen die Stadtwerke nur geringe Datenraten, aber hohe Gerätekapazität pro Zelle. Eine hohe Datenrate können hingegen Netzbetreiber gut brauchen, zum Beispiel um an Hotspots zahlreiche Kunden zu versorgen . Auch kann man so mehrere Kunden über stationäre 5G-Internetanschlüsse mit glasfaserähnlichen Geschwindigkeiten versorgen (Fixed Wireless Access, FWA).

Die hohe Skalierbarkeit ist erst ab Ende 2021 in fertigen Geräten zu erwarten und die Spitzendatenrate von 10 GBit/s noch später (nachdem mmWave-Frequenzen versteigert worden sind). Campusnetze werden allerdings schon heute benötigt, weil WLAN nicht mehr für alle Aufgaben ausreicht.