Editorial

Liebe Leserin, lieber Leser,

die Entwicklungen in der IT-Welt sind so rasant, dass es selbst Profis nicht immer leichtfällt, das eigene Know-how auf einem aktuellen Stand zu halten. Zudem gibt es immer mehr Themen, bei denen kaum noch jemand sagen kann: Mythos oder Wahrheit? Und gar nicht so selten lautet die Antwort darauf auch: Es kommt darauf an.

In diesem Sonderheft nehmen wir Sie darüberhinaus mit auf eine Reise zu spannenden Fakten über künstliche Intelligenz. Tauchen Sie ein in Denkmuster und Mechanismen, die hinter dieser faszinierenden Welt stecken, und erfahren Sie, wie Sie Bildgeneratoren manipulieren können und wie KI Emotionen erkennt. Außerdem bietet Ihnen diese Ausgabe Einblicke in Innovationen, die unsere Zukunft formen werden.

Dass sich tiefschürfender Lesestoff und Kurzweil nicht ausschließen, zeigen unsere Beispiele, in denen Sie erfahren, wie Sie QR-Codes ohne Smartphone entschlüsseln, wie Sie Daten des James-Webb-Teleskops selbst auswerten und wie Sie lernen, Zauberwürfel systematisch zu lösen – nicht mit Magie, sondern mit Algorithmen. Zu guter Letzt geht es weit zurück in die Vergangenheit: Hätten Sie gewusst, wie lange es gedauert hat, bis historische Geheimschriften dechiffriert wurden und wie sie noch heute auf moderne Verschlüsselungsverfahren nachwirken?

Wir wünschen Ihnen viel Spaß und Neugier beim Lesen unserer Artikel – und dass Sie künftig in Gesprächen mit noch mehr nerdigem Fachwissen glänzen können.

Anke Brandt

Inhalt

IT-MYTHEN ENTZAUBERT

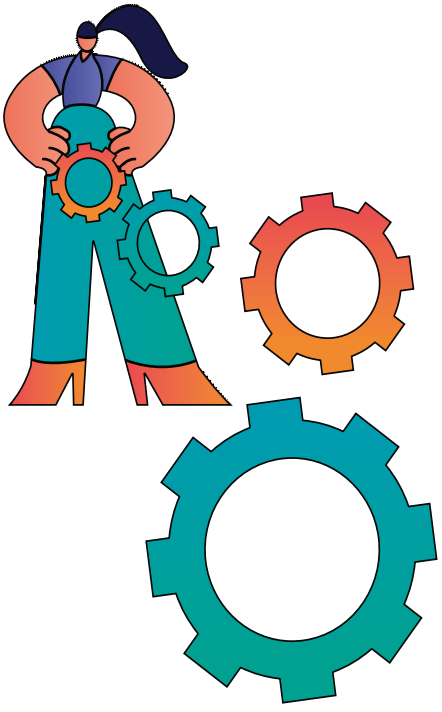
Stimmt es eigentlich, dass KI so stromhungrig ist, wie man es immer wieder hört? Und was ist dran am Gerücht, dass jeder Drucker nicht sichtbare Codes mitdruckt? Wir prüfen verbreitete Mythen über Nachhaltigkeit in der IT-Welt, Betriebssysteme, Sicherheit und Hardware.

SO FUNKTIONIERT KI

Welche Denkmuster hinter künstlicher Intelligenz stecken oder dass sie Emotionen erkennen kann, wissen vermutlich nur wenige. Genauso, dass sich Bildgeneratoren manipulieren lassen, sodass sie einen Hund für eine Katze halten.

SPANNENDES AUS DER FORSCHUNG

Ein kuratierter Mix aus der bunten Welt der Wissenschaft: Lauschende Autos und winzige künstliche Nasen, die Gasmoleküle erschnuppern, kommen darin genauso vor wie das James-Webb-Teleskop, dessen Daten Sie sogar selbst auswerten können.



NERDWISSEN ERKLÄRT

Zauberwürfeln auf den Grund gehen, einen KI-Rapper basteln oder QR-Codes per Hand dechiffrieren – bei diesen Themen muss man sich nicht auskennen, will man aber. Wer sich für spezielles Wissen zu nerdigen Themen interessiert, ist hier genau richtig.

HISTORISCHE VERSCHLÜSSELUNGEN KNACKEN

Alte Verschlüsselungen spielen heute zwar keine Rolle mehr, dienen aber trotzdem als gutes Lehrbeispiel, um in die Welt der Kryptografie einzutauchen. Manche waren ihrer Zeit weit voraus und wurden erst nach Hunderten von Jahren dechiffriert.

ZUM HEFT

IT-Mythen im c’t-Check

Laser- oder Tintendrucker? Linux, macOS oder Windows? Zu solch grundsätzlichen Fragen geistern oft einfache Antworten herum, die sich bei näherem Hinsehen aber gern mal als falsch entpuppen. Auf den folgenden Seiten räumen wir mit populären IT-Mythen auf.

Von **Greta Friedrich**

Bild: Andreas Martini

Wenn es um Computertechnik geht, sind viele Menschen Experten – oder glauben das zumindest. Schließlich nutzen sie täglich Smartphone, Notebook und den PC am Arbeitsplatz, geben Passwörter ein und bezahlen digital. In Gesprächen sind technische Finessen daher ein häufiges Thema, ob in der Familie, im Büro oder im Freundeskreis. So verbreitet sich jedoch nicht nur Wissen, sondern auch Fehleinschätzungen halten sich hartnäckig.

Einige gängige Behauptungen wollen wir in den folgenden Artikeln untersuchen. Nicht zum ersten Mal schauen wir in die IT-Gerüchteküche [1, 2, 3], doch manche Mythen sind einfach nicht totzukriegen und andere entstehen neu. So stellt sich mit dem aktuellen KI-Hype die Frage, ob die Technik ein Energiefresser ist – wir antworten weiter unten. Für den IT-Mythen-Check haben wir aus dem weiten Themenfeld die Bereiche Nachhaltigkeit, Betriebssysteme, Sicherheit und Hardware ausgewählt. Um Ihnen einen schnellen Überblick zu geben, haben wir die Mythen jeweils mit einem Pfeil versehen: ↑ für wahr, ↓ für falsch und → für „kommt drauf an".

Gleich nach dieser kurzen Einleitung geht es um Fragen der Nachhaltigkeit, etwa: „Ist Streaming klimaschädlicher als CDs oder DVDs?" und „Was ist ökologischer, ein Mini-PC oder ein Notebook?". Es folgt der Abschnitt Betriebssysteme (siehe Artikel „Mythen zu Windows und Linux"), der unter anderem erklärt, ob eines der beiden Systeme sicherer ist als das andere.

Das Kapitel Sicherheit (siehe Artikel „Sicherheitsmythen beleuchtet") umfasst Themen wie Passwörter, digitales Bezahlen, anonymes Surfen und Smart-TVs. Den Abschluss bildet der Bereich Hardware (siehe Artikel „Hardware-Mythen von Drucker bis WLAN"): Hier geht es um Glauben und Aberglauben zu der Alterung von SSDs, der Effizienz von Prozessoren und den Druckkosten von Laserdruckern. Ob letztere tatsächlich über Ausdrucke identifiziert werden können, beantworten wir ebenfalls.

Nach der Lektüre können Sie bestimmt den einen

man streamt. Das Rechenzentrum, die Datenübertragung und das Endgerät benötigen Energie, beeinflusst auch von der Abspielqualität. Für eine CO_2-Bilanz des Streamings muss man außerdem den jeweiligen Strommix berücksichtigen und den gesamten Lebenszyklus der genutzten Server, Leitungen und Geräte. Allgemeingültige Zahlen zu erheben, ist daher kaum möglich [4] – einige klare Anhaltspunkte gibt es dennoch.

Beim Endgerät gilt: Je größer der Bildschirm, desto mehr Energie ist nötig. Hier ist also das Smartphone die energiesparsamste Wahl, dicht gefolgt von Tablet und Laptop. Fernseher dagegen brauchen deutlich mehr Energie; laut einem Hintergrundpapier des Borderstep-Instituts von 2020 [5] ist es daher zum Beispiel energiesparender, in SD-Auflösung auf einem kleinen Bildschirm zu streamen, als auf einem 50-Zoll-Fernseher eine DVD abzuspielen oder lineares Fernsehen zu sehen.

Je höher die Qualität von Audio und Video, desto energieintensiver ist das Streaming. Laut dem Borderstep-Institut benötigt man für eine Stunde Videostreaming im Festnetz in niedriger HD-Qualität (720p) auf einem 65-Zoll-Fernseher circa 280 Wattstunden an Energie. Das entspräche CO_2-Emissionen von circa 130 Gramm, also in etwa dem, was ein sparsamer Mittelklassewagen laut ADAC auf nur einem Kilometer Fahrt ausstößt. In 4K-Videoqualität sei auf demselben Gerät mehr als viereinhalbmal so viel Energie nötig, so Borderstep. Der Mehraufwand entsteht vor allem bei Netzen und Rechenzentren, denn mit der Auflösung steigt auch die Datenrate (und die Datenmenge insgesamt).

Auch der Weg, den die Daten vom Server auf das Endgerät nehmen, beeinflusst den Streaming-Energieaufwand enorm. Optimalerweise streamt man über das Festnetz, also im WLAN oder per LAN-Kabel. Übers Mobilfunknetz ist deutlich mehr Energie nötig – das gilt zum Beispiel auch für das WLAN in Zügen, denn dort wird der Internetzugang über den Mobilfunk hergestellt. Anders ist es etwa beim ICE-

Transformer: Sprach-KI mit Aufmerksamkeit

Nicht jede KI wird schlauer, wenn man sie auf gigantische Ausmaße aufbläst – der Textgenerator GPT-3 hingegen schon. Wir zeigen, wie die dahinter liegende Transformer-Technik funktioniert.

Von **Pina Merkert**

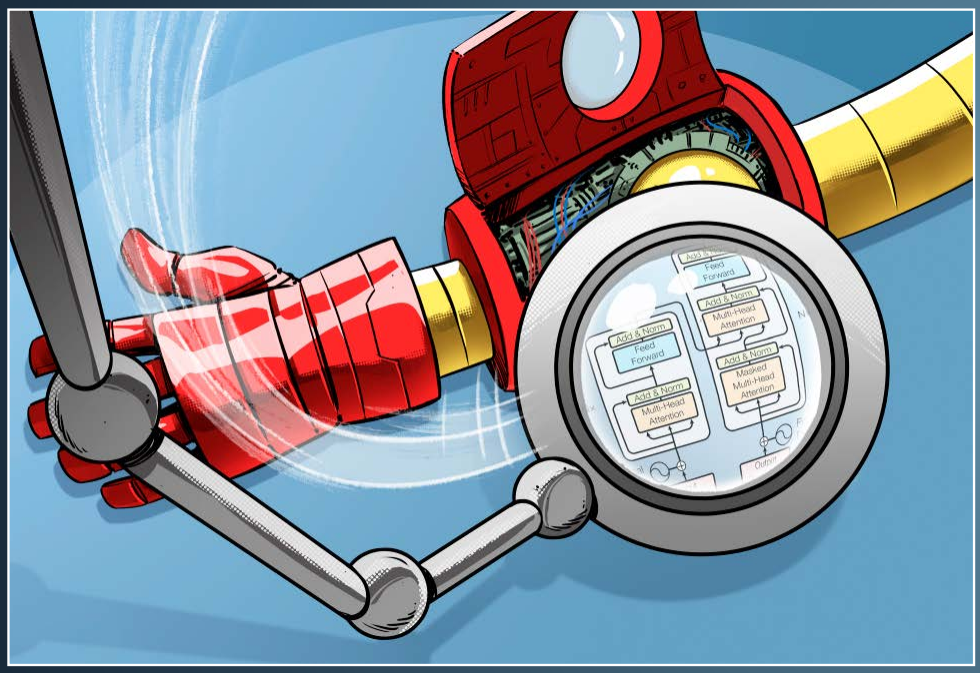


Bild: Albert Hulm

Transformieren meint ganz allgemein das Umwandeln von einem in etwas anderes. Im Kontext von KI bedeutet „Transformer“ eine ganz bestimmte Architektur für neuronale Netze, die in den letzten Jahren ganz groß herauskam, sowohl bezogen auf den Umfang als auch auf die Verbreitung der Sprachmodelle. Diese neuronalen Netze transformieren Sätze in Bedeutungssequenzen. Aus denen können Netze mit der gleichen Struktur auch wieder Sätze berechnen.

Die 2017 von Google-Forschern vorgestellten Transformer lernen in ihrer Trainingsphase nicht nur, wie sie die Daten verarbeiten, sondern auch, worauf sie ihre Aufmerksamkeit richten müssen. Aufmerksamkeit und Datenverarbeitung stecken zusammen in Blöcken, die sich leicht zu tiefen Netzen stapeln lassen. Deswegen gelingt es, Transformer massiv zu skalieren, beispielsweise zu riesigen Sprachmodellen wie GPT-3 von OpenAI mit 175 Milliarden Parametern. Den Konkurrenten BERT mit 110 Millionen Parametern kann man noch daheim auf einer dicken Grafikkarte trainieren, für GPT-3 braucht man ein Rechenzentrum und gute Nerven, wenn die Stromrechnung kommt.

Was GPT-3 kann und wie Sie es selbst nutzen, haben wir in [1, 2] beschrieben. Dieser Artikel beleuchtet die Details, die Transformer zu so raffinierten Schreibern machen. Machen Sie sich allerdings auf einen wilden Ritt gefasst, denn Transformer nutzen nicht nur viele Tricks bekannter neuronaler Netze [3], sondern satteln noch mehrschichtig und mehrköpfig Aufmerksamkeit drauf.

Wir versuchen dabei alle mathematischen Tricks zu nennen, um es Ihnen leichter zu machen, wenn Sie das Forschungspaper mit allen Formeln lesen wollen. Für die Einordnung am Ende des Artikels müssen Sie aber nicht jedes Detail komplett durchschaut haben, es reicht, wenn Sie hie und da ein Gefühl dafür bekommen, wie das System funktioniert. Denn auch die Erfinder der Transformer wissen nicht genau, welche Parameter an welcher Stelle

Die Bedeutung von Wörtern ist aber kontextabhängig. Je nachdem, ob der Satz „Ich möchte die Bank“ mit „streichen“ oder mit „überfallen“ endet, hat er eine komplett andere Bedeutung. Sprach-KIs verarbeiten daher schon seit vielen Jahren die komplette Sequenz an Eingaben, stellen sie intern als sogenannten „Latent Vector“ dar und berechnen aus diesem Vektor wieder die Ausgaben. OpenAI nennt diesen Vektor bei GPT-3 „Embedding“.

Embedding-Vektoren

Statt mit ganzen Wörtern arbeiten Sprach-KIs meist mit „Tokens“. Die repräsentieren ganze Wörter oder auch nur Wortteile, Satzzeichen sowie die Spezialsymbole „Ende“ und „Auslassung“. Jede Sprach-KI nutzt ihre eigene Liste aus einigen Tausend Tokens und bringt sie in ein einheitliches Format. Damit muss sich die KI schon mal nicht mehr mit Buchstaben herumschlagen.

Neuronale Netze funktionieren am besten mit Eingabevektoren, wenn deren Werte zwischen 0 und 1 liegen. Zu solchen Vektoren kommt man mit einer Tabelle, die sich effizient als Matrix darstellen lässt. Die Werte in der Matrix initialisieren die Forscher mit Zufallszahlen, sodass jedes Wort einen anderen Vektor bekommt. Zufällige Vektoren sind aber nicht gut darin, die Bedeutung von Wörtern darzustellen. Deswegen lassen die Forscher die Werte in kleinen Schritten mit dem gleichen Gradientenabstiegsalgorithmus anpassen, der auch die Parameter der neuronalen Netze trainiert. In vielen Trainingsschritten bilden sich dann bedeutungsvolle Vektoren heraus. Man kann Embedding-Vektoren und die Synapsengewichte (auch „Parameter“ genannt, siehe [3]) des neuronalen Netzes sogar gemeinsam trainieren.

Die gelernten Vektoren für jedes Wort bezeichnet man normalerweise als „Word Embeddings“. Achtung, es besteht Verwechslungsgefahr mit OpenAIs „Embedding“ zwischen Encoder und Decoder (dazu

Das Auto lernt, auf Signale zu hören

Moderne Autos nutzen längst Kameras, aber noch keine Audiosensoren. Forscher testen Mikrofone und Audio-KI am Fahrzeug. Die orten Einsatzfahrzeuge, die sich mit Martinshorn nähern, nehmen abgenutzte Bremsbeläge wahr und erkennen Sprachbefehle, etwa zum Öffnen des Kofferraums.

Von **Arne Grävemeyer**

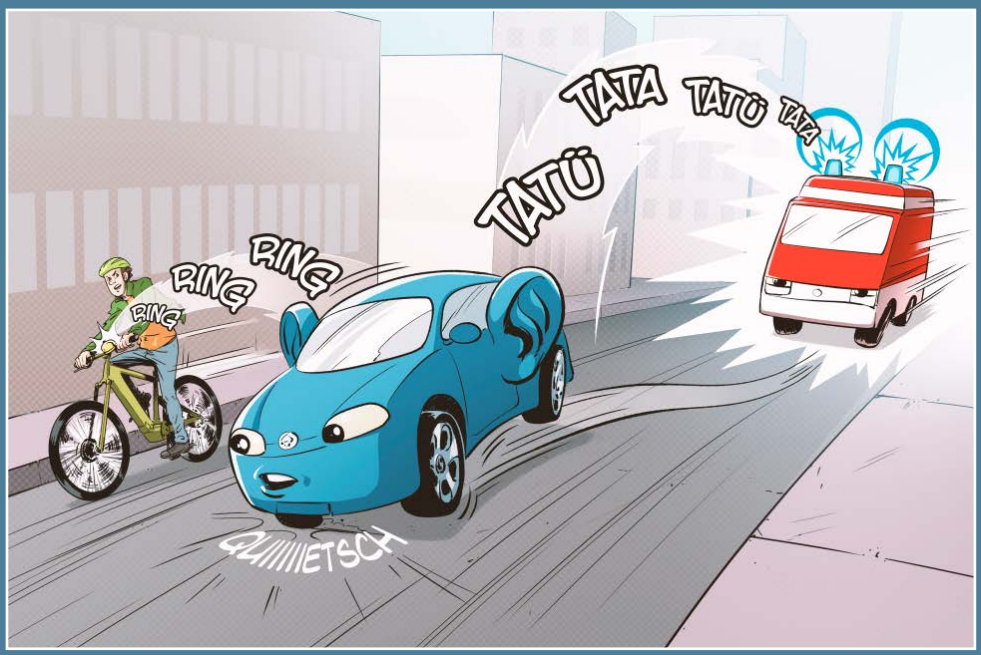


Bild: Albert Hulm

Die Zahl der Fahrassistenzsysteme in Pkw ist in den vergangenen Jahren schnell gestiegen. Kameras und Lidar helfen heute beim Einparken; sie registrieren, wenn der Wagen die Spur verlässt oder der Abstand zum Vordermann zu knapp wird. Mit der fortschreitenden Entwicklung autonomer Fahrzeuge wird voraussichtlich die Zahl der Außensensoren weiter steigen, damit die Systeme Verkehrssituationen möglichst vollständig erfassen können.

Anders als menschliche Fahrer, die in vielen Situationen nicht nur ihren Augen vertrauen, sondern auch auf Geräusche achten, haben heutige Serienfahrzeuge keinen Sinn für akustische Hinweise. Die einzige Ausnahme bildet vielleicht ein Mikrofon für Sprachbefehle im Innenraum. Das wollen Forscher um Moritz Brandes am Fraunhofer-Institut für digitale Medientechnologie (IDMT) in Oldenburg mit ihrem Projekt „The Hearing Car“ ändern.

Martinshorn schnell erfasst

Ein wichtiges Beispiel ist die Alltagssituation, in der sich ein Rettungswagen mit hoher Geschwindigkeit von hinten nähert und mit Martinshorn und Blaulicht auf sich aufmerksam macht. Autofahrer sind verpflichtet, solchen Einsatzfahrzeugen ohne zu zögern Vorrang einzuräumen. Oft hören Autofahrer die Sirene deutlich früher, als dass ihnen das Blaulicht auffällt. Was aber, wenn das Radio spielt und sich zusätzlich die Reisenden im Innenraum unterhalten? Dann wäre es hilfreich, wenn das Auto mit eigenen Sensoren das herannahende Martinshorn erkennen und den Fahrer über das Infotainment-System darauf hinweisen könnte. Überdies verlangt das Gesetz zum autonomen Fahren von 2021, dass auch autonome Fahrzeuge im Notfall einem Einsatzfahrzeug ebenso unverzüglich wie ein menschlicher Fahrer Platz machen müssen.

„Die Sirenenerkennung ist der wichtigste Türöffner für Außenmikrofone am Auto. Zu dieser Funktion erhalten wir die meisten Anfragen aus der Industrie“, berichtet Brandes. Tatsächlich haben die Ingenieure aus Oldenburg zuerst Versuche unternommen, mit dem Mikrofon im Fahrzeuginnenraum auch die typische Sirene eines herannahenden Martinshorns zu erfassen und mittels einer darauf trainierten künstlichen Intelligenz in der Audiospur zu erkennen. Aber übliche Fahrgeräusche im Innenraum beziehungsweise dessen Schalldämmung, dazu Radiomusik und Gespräche machten die Erkennung mit der vorhandenen Audiotechnik viel zu unsicher.

Ein Mikrofon am Fahrzeugheck dagegen liefert wesentlich klarere Informationen über akustische Signale von hinten. Für die Erkennung unterschiedlicher Ereignisse haben die Forscher eine KI trainiert. Dazu unterteilen sie den aufgenommenen Stream in Blöcke von wenigen Millisekunden Dauer. Zu jedem dieser Blöcke liefert die KI eine Einzelentscheidung. Diese Einschätzungen summieren sich dann über die Zeit zu Tendenzen auf, bestärken sich gegenseitig oder widersprechen einander. Nach etwa einer halben Sekunde kann der KI-Erkenner bereits mit ziemlicher Sicherheit entscheiden, ob er ein Martinshorn gehört hat oder nicht.

Derselbe Erkenner des Fraunhofer IDMT kann inzwischen auch andere Geräuschquellen unterscheiden. Dazu zählen Autohupen, Fahrradklingeln,

Bild: IDMT/Anika Bödecker

God's Number für den Zauberwürfel

Als sich Mathematiker 1980 fragten, wie viele Züge es maximal braucht, um jeden Zauberwürfel zu lösen, wussten sie noch nicht, dass sie 30 Jahre an der Antwort zu kauen haben. Wir tauchen ein in die Welt der Zauberwürfel und erzählen, wie die Mathematiker es letztlich geschafft haben, diese Zahl zu bestimmen.

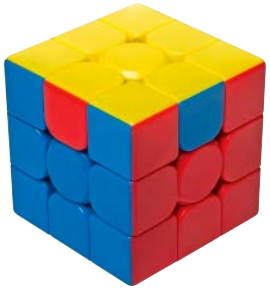
Von **Wilhelm Drehling**

Ein verdrehter Zauberwürfel sieht auf den ersten Blick wie eine unlösbare Aufgabe aus. Jede Bewegung einer Ebene orientiert die Teile eines Würfels neu und verschiebt dafür andere. Schon nach wenigen Verdrehungen verliert man den Überblick. Die schiere Anzahl an möglichen Kombinationen motivierte Mathematiker, den Rubik's Cube zu erforschen und sich folgende Frage auszudenken: Angenommen, Gott ist in der Lage, jeden Zustand eines Würfels immer perfekt zu lösen. Wie viele Bewegungen der Ebenen bräuchte er maximal, um jeden beliebigen Zustand des Zauberwürfels lösen zu können? Die Zahl tauften die Mathematiker „God's Number".

Während Speedcuber den Würfel in der kürzesten Zeit lösen wollten, interessierte Mathematiker die theoretische Version der Frage. Wie viele Drehungen reichen, wenn Gott keine Fehler macht? Was sie damals noch nicht wussten: Die Suche nach God's Number entpuppte sich als überhaupt nicht trivial und beschäftigte Mathematiker rund um die Welt 30 Jahre lang. Erst 2010 fanden Tomas Rokicki, Herbert Kociemba und Morley Davidson endlich die Lösung.

Der Begriff God's Number oder auch Gottes Algorithmus wurde zwar für den Zauberwürfel geprägt, tritt aber auch in anderen Spielen und Puzzles auf, wenn eine kleinstmögliche optimale Lösung vorhanden ist. Beim Schach zum Beispiel gibt es die sogenannten Tablebases: Alle möglichen Positionen mit sieben Figuren oder weniger sind gelöst. Es gibt also für alle diese Fälle eine optimale Lösung, die entweder zum Sieg, zum Unentschieden oder zur unweigerlichen Niederlage führt. Wer jetzt glaubt, seine Freunde im Endspiel in Grund und Boden spielen zu können, sollte Platz auf seinem Rechner schaffen, denn die Tablebases umfassen mehr als 16 TByte an Festplattenspeicher. Doch das ist gar nichts im Unterschied zu der möglichen Anzahl an Zuständen, die ein Zauberwürfel annehmen kann.

43 Trillionen



Wenn nur zwei Kanten oder nur zwei Ecken miteinander vertauscht sind, ist der Würfel nicht mehr lösbar.

gical Society of America hat angenommen, dass auf dem Planeten Erde zu jeder Zeit etwa 10 Trillionen Insekten leben: Es gibt also etwa viermal so viele Zauberwürfelzustände wie Insekten auf der Welt.

Wie kommen die 43 Trillionen zustande? Um sie zu berechnen, müssen Sie sich vorstellen, wie ein Zauberwürfel aufgebaut ist: Es gibt acht Eckteile mit drei Farben und 12 Kanten mit zwei Farben, außerdem noch sechs einfarbige Mittelsteine, die ihren Platz nicht verlassen.

Die Anzahl der möglichen Positionen für Ecken und Kanten berechnen Sie mithilfe von Permutation – die kennt man aus der Wahrscheinlichkeitstheorie. Die erste Ecke kann sich an acht Positionen befinden, die nächste nur noch an sieben, weil die erste ja einen möglichen Platz belegt. Die Ecke danach kann an sechs möglichen Plätzen sein und so weiter. Das entspricht $8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 8!$ Möglichkeiten für die Ecken und 12! für die Kanten. Da jede Ecke zusätzlich noch in drei unterschiedlichen Weisen verdreht sein kann, muss man diese schon große Zahl noch mit 3^8 multiplizieren, das gleiche Spiel bei den Kanten (2^{12}). Zusammengerechnet ergibt das $8! \cdot 3^8 \cdot 12! \cdot 2^{12} = 519.024.039.293.878.272.000$ Möglichkeiten, was überraschenderweise sehr viel grö-

Nachrichten aus dem Vatikan dechiffriert

Kryptografie ist keine Erfindung des Computerzeitalters, und im 16. Jahrhundert war der Vatikan Vorreiter bei der sicheren Datenübertragung. Um dessen Nachrichten zu entschlüsseln, arbeiten heute Informatiker, Kryptologen, Linguisten und Historiker zusammen und stellen fest: Schon ab dem 18. Jahrhundert hatte der Vatikan Fachkräftemangel. Wir zeichnen Geschichte nach.

Von **Nils Kopal und Beáta Megyesi**

Bild: Albert Hulm

Schon kurz nach der Erfindung der Schrift entwickelten Menschen das Bedürfnis, wichtige geschriebene Informationen so zu verbergen, dass nur bestimmte Empfänger sie lesen können. Innerhalb der letzten viertausend Jahre entwickelte sich daher die Kryptografie, also die Wissenschaft und Kunst des geheimen Schreibens, stetig weiter. Heute liegen viele historische, teilweise mehrere Hundert Jahre alte und rätselhaft verschlüsselte Dokumente in Archiven über die ganze Welt verteilt – zum Beispiel im Vatikanischen Apostolischen Archiv (das früher Geheimarchiv hieß) oder im Haus-, Hof- und Staatsarchiv in Wien. Experten gehen davon aus, dass – selbst wenn nur ein Prozent aller archivierten Dokumente verschlüsselt sind –, diese zusammengenommen Hunderte Meter Archivgänge füllen würden; ein großer Teil dieser Dokumente ist bis heute nicht entschlüsselt worden.

Viel Arbeit für die Kryptoanalytiker – die natürlichen Gegenspieler der Kryptografen – die sich ums Entschlüsseln von verschlüsselten Texten bemühen. Und deren Arbeit wird zusätzlich erschwert: Zumeist sind die verschlüsselten historischen Dokumente nicht zentral archiviert, nicht digital zugänglich, über verschiedene Regale und Boxen in den Archiven verstreut und müssen von interessierten Forschern zunächst mühsam zusammengetragen werden. Immer wieder stolpern Historiker über verschlüsselte Dokumente, können aber wenig damit anfangen, weil Entschlüsselung nicht zu ihren geübten Tätigkeiten gehört.

Das DECRYPT-Projekt

Das Entschlüsseln historischer Texte ist eine interdisziplinäre Aufgabe, die weder Historiker noch Informatiker allein bewältigen können. Zu gemeinsamen Erfolgen verhelfen das DECRYPT-Projekt und sein Vorgänger namens DECODE. Ziel der Forschungszusammenarbeit ist, historische Kryptologie in großem Umfang systematisch und interdisziplinär zu erforschen. Geleitet wird das Projekt aus Uppsala in Schweden. Ein Team aus Historikern, historischen und Computer-Linguisten, Philologen, Informatikern und Kryptologen aus Deutschland, Frankreich, Großbritannien, Israel, den Niederlanden, der Slowakei, Spanien und Ungarn arbeitet gemeinsam an dem Ziel, die verschlüsselte Vergangenheit in Form von originalen Dokumenten zusammenzutragen. Mithilfe von computergestützten Methoden werden sie analysiert und die Ergebnisse einer breiten Öffentlichkeit verständlich nähergebracht. Alle im Projekt erarbeiteten Datensammlungen, Werkzeuge und Ergebnisse stellen sie anderen Forschern für ihre Arbeit mit verschlüsselten Dokumenten zur Verfügung (siehe ct.de/wg7q). Die Herausforderungen, denen sich die Forscher stellen, sind vielfältig: Zunächst müssen Historiker die verschlüsselten Dokumente in den Archiven ausfindig machen und digitalisieren, zum Beispiel durch Fotografieren oder Scannen.

Die rätselhaften Dokumente, die im Vatikan und anderen europäischen Archiven liegen, werden bei DECRYPT in der zentralen Datenbank DECODE gesammelt. Die Datenbank mit den Metadaten selbst steht öffentlich im Internet, zu finden über ct.de/wg7q. Aus rechtlichen Gründen sind die gescannten Dokumente selbst nicht immer online einsehbar. Die Sammlung enthält mittlerweile mehr als 2500 Manuskripte von einer Seite Länge bis zur Länge eines ganzen Buchs.

Kryptografie, Kryptologie und Kryptoanalyse

Drei Begriffe tauchen rund um Verschlüsselung auf, die keine Synonyme sind. **Kryptologie** ist der Oberbegriff für die wissenschaftliche Auseinandersetzung mit Ver- und Entschlüsselung von Nachrichten. Histo-