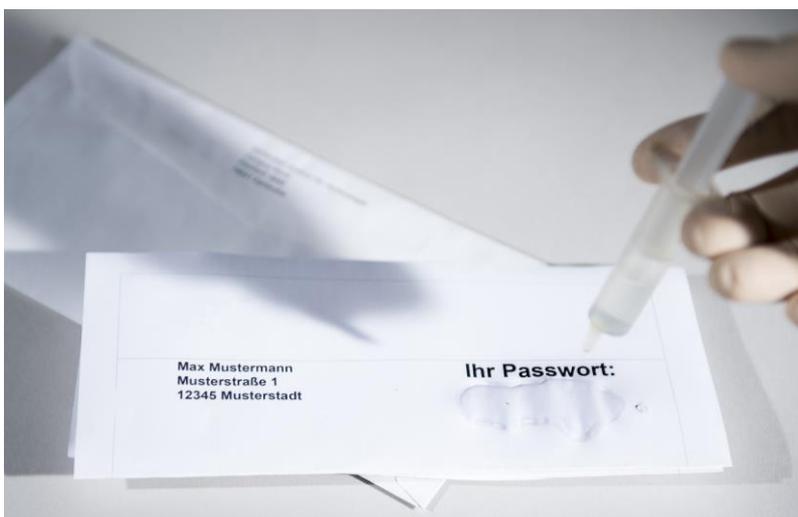


Agent 007: Organische Moleküle als Geheimnisträger

Wissenschaftler des KIT designen chemische Verbindungen, die als Passwörter für verschlüsselte Informationen eingesetzt werden können – Veröffentlichung in *Nature Communications*



Unsichtbares Passwort: Die Information für die Verschlüsselung steckt im Molekül, zum Beispiel als Flüssigkeit auf Papier aufgetropft. (Foto: Amadeus Bramsiepe, KIT)

Im Zeitalter digitaler Übertragung ist der Schutz sensibler Informationen ein überaus wichtiges Thema. Viele Daten werden daher verschlüsselt auf die Datenautobahn geschickt. Zumeist verwenden diese Verfahren zum Entschlüsseln ein Passwort, und genau dieses ist in den allermeisten Fällen die Eintrittspforte für Codeknacker. Einen neuen und sehr sicheren Weg wählten Wissenschaftlerinnen und Wissenschaftler des Karlsruher Instituts für Technologie (KIT), indem sie Informatik mit Chemie paarten und ein gängiges Verschlüsselungsverfahren mit einem chemischen Passwort kombinierten. Über ihre Entwicklung berichten sie nun in einer Open Access Publikation in *Nature Communications*. (DOI: 10.1038/s41467-018-03784-x).

Bereits jetzt existieren sehr gute und effektive Verschlüsselungsprogramme, die fast nicht zu überwinden sind, vorausgesetzt die Rechnerleistung ist begrenzt. Schwachstelle bleibt dabei immer das Passwort. Wenn es schlecht gewählt ist und nicht den nötigen Sicherheitsansprüchen genügt, bildet es die Achillesferse der gesamten Verschlüsselung. Genau an dieser Stelle setzen die Wissenschaftler des

Monika Landgraf
Pressesprecherin,
Leiterin Gesamtkommunikation

Kaiserstraße 12
76131 Karlsruhe
Tel.: +49 721 608-21105
E-Mail: presse@kit.edu

Weiterer Pressekontakt:

Regina Link
Redakteurin/Pressereferentin
Tel.: +49 721 608-21158
E-Mail: regina.link@kit.edu

Weitere Materialien:

Originalpublikation:
<https://www.nature.com/articles/s41467-018-03784-x>

KIT an: Sie verbergen die Information für das Passwort in einem kleinen organischen Molekül. Und während die verschlüsselte digitale Information dann gewissermaßen öffentlich reisen kann, wird der Schlüssel zum Lesen der Information unsichtbar und ohne Wissen der Umwelt in Form einer kleinen Menge der chemischen Verbindung, beispielsweise aufgetropft auf Papier, transportiert.

„Das Verfahren eignet sich natürlich nur für Anwendungen, die eine sehr hohe Sicherheitsstufe benötigen und damit auch einen gewissen Aufwand rechtfertigt, etwa für die Übermittlung von Geheimdienstinformationen oder bei der Kommunikation in Botschaften“, so Professor Michael Meier vom Institut für Organische Chemie. Auch um Plagiate von Originalen zu unterscheiden oder Produktinformationen wie Charge oder Produktionsdatum fälschungssicher am Produkt anzubringen, bietet sich das Verfahren an. „Wir können mit geringsten Mengen arbeiten und finden diese auch in Materialien, bei denen man mit anderen chemischen Verbindungen, etwa DNA-Molekülen, nicht weit kommt“, so Erstautor Andreas Boukis. So gelang es den Wissenschaftlern, die chemischen Schlüssel aus unterschiedlichen Trägermaterialien, beispielsweise Papier, Parfüm, Instantkaffee, Grüner Tee, Zucker oder sogar Schweineblut mit hoher Zuverlässigkeit zu isolieren.



Auftropfen, versenden, entschlüsseln: Was hier vereinfacht dargestellt ist, ist ein sehr komplexes – und sehr sicheres – Verfahren. (Fotos: Amadeus Bramsiepe, KIT; Grafik: Leon Kühner, KIT)

Die Information des chemischen Schlüssels steckt in der Abfolge seiner Bausteine und den daran angehängten Seitenketten. Jeder dieser chemischen Komponenten erhält einen Buchstaben und eine Ziffer zugewiesen, es ergibt sich dadurch, je nachdem welche Bausteine in gegebener Reihenfolge und mit welchen Seitenketten synthetisiert werden, ein individueller alphanumerischer Code für das Passwort-

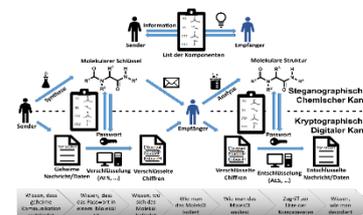
Molekül, der mit einem eigens dafür entwickelten Computerprogramm ausgelesen und in einen binären Code umgewandelt wird. Für die Synthese verwendeten die Wissenschaftler eine gängige sogenannte Multikomponentenreaktion. Diese ermöglicht es, verhältnismäßig unaufwendig in einem Schritt ein zuvor definiertes Molekül zu synthetisieren. Als einzelne Grundbausteine wählten die Forscher geeignete kommerziell erhältliche Verbindungen. Mit dieser Bibliothek aus 130 verschiedenen Grundbausteinen lassen sich 500.000 chemische Schlüssel synthetisieren, die jeweils eine Grundinformation von 18 Bit enthalten. Durch die Kombination verschiedener chemischer Schlüssel, die auch zeitlich und örtlich unterschiedlich übermittelt werden können, lässt sich die Informationsspeichergröße und damit die Sicherheit weiter erhöhen. Da die Verbindungen sehr robust sind, eignen sie sich für viele unterschiedliche Trägermaterialien. Dank einer weiteren Eigenschaft sind sie zudem leicht zu finden: Sie tragen in einer Position eine besondere Seitenkette, welche die Rückgewinnung erleichtert, sogenannte Perfluoralkyle. Diese haben ähnliche Eigenschaften wie Teflon, das heißt sie wechselwirken nicht gerne mit wässrigen (polaren) oder fetthaltigen (unpolaren) Medien, sondern nur mit anderen perfluorierten Verbindungen, darum kann man diese Moleküle selektiv aus einem Gemisch abtrennen. Die Analyse der isolierten Verbindungen geschieht im Anschluss mit einer gängigen, hochsensiblen Analyseverfahren, der Massenspektrometrie. Dabei wird die Masse ganzer Moleküle, aber auch die definierter Bruchstücke bestimmt. Kennt man die Bibliothek der 130 möglichen Ausgangskomponenten, lässt sich so auf das Molekül rückschließen und man kann dann das Passwort zum Entschlüsseln ablesen.

„Die Idee, Informationen über geheime Kanäle zu schicken, ist nicht neu, unser Verfahren zeichnet aber aus, dass wir einen besonders robusten geheimen Kanal zur Verfügung stellen, welcher mit minimalen Mengen an Schlüssel-molekül auskommt,“ fasst Professor Dennis Hofheinz vom Institut für Theoretische Informatik die Vorteile der chemischen Passwörter zusammen.

Entwickelt wurde das neue Verfahren im Rahmen des Sonderforschungsbereiches (SFB) 1176 „Molekulare Strukturierung weicher Materie“ der Deutschen Forschungsgemeinschaft (DFG), der vom KIT koordiniert wird. Neun Millionen Euro stehen dem im Januar 2016 gestarteten SFB in den ersten vier Jahren zur Verfügung.

Originalpublikation:

A. C. Boukis, K. Reiter, M. Frölich, D. Hofheinz und M. A. R. Meier: *Multicomponent reactions provide key molecules for secret communication. Nature Communications, 2018. doi:10.1038/s41467-018-03784-x.*



Informatik trifft Chemie: Ver- und Entschlüsselung im Detail. (Grafik: Andreas Boukis, KIT)

<https://www.nature.com/articles/s41467-018-03784-x>

Als „Die Forschungsuniversität in der Helmholtz-Gemeinschaft“ schafft und vermittelt das KIT Wissen für Gesellschaft und Umwelt. Ziel ist es, zu den globalen Herausforderungen maßgebliche Beiträge in den Feldern Energie, Mobilität und Information zu leisten. Dazu arbeiten rund 9 300 Mitarbeiterinnen und Mitarbeiter auf einer breiten disziplinären Basis in Natur-, Ingenieur-, Wirtschafts- sowie Geistes- und Sozialwissenschaften zusammen. Seine 26 000 Studierenden bereitet das KIT durch ein forschungsorientiertes universitäres Studium auf verantwortungsvolle Aufgaben in Gesellschaft, Wirtschaft und Wissenschaft vor. Die Innovationstätigkeit am KIT schlägt die Brücke zwischen Erkenntnis und Anwendung zum gesellschaftlichen Nutzen, wirtschaftlichen Wohlstand und Erhalt unserer natürlichen Lebensgrundlagen.

Das KIT ist seit 2010 als familiengerechte Hochschule zertifiziert.

Diese Presseinformation ist im Internet abrufbar unter:
www.sek.kit.edu/presse.php

Das Foto steht in der höchsten uns vorliegenden Qualität auf www.kit.edu zum Download bereit und kann angefordert werden unter: presse@kit.edu oder +49 721 608-21105. Die Verwendung des Bildes ist ausschließlich in dem oben genannten Zusammenhang gestattet.