Schulze, Matthias

Research Report

Homomorphe Verschlüsselung und Europas Cloud: Ein Baustein für Europas digitale Souveränität

SWP-Aktuell, No. 15/2021

Provided in Cooperation with:
Stiftung Wissenschaft und Politik (SWP), German Institute for International and Security Affairs, Berlin

Suggested Citation: Schulze, Matthias (2021) : Homomorphe Verschlüsselung und Europas Cloud: Ein Baustein für Europas digitale Souveränität, SWP-Aktuell, No. 15/2021, Stiftung Wissenschaft und Politik (SWP), Berlin, https://doi.org/10.18449/2021A15

SWP

SWP-Aktuell

NR. 15 FEBRUAR 2021

Homomorphe Verschlüsselung und Europas Cloud

Ein Baustein für Europas digitale Souveränität

Matthias Schulze

Homomorphe Verschlüsselung stellt einen nächsten Evolutionsschritt der Kryptografie dar. Mit dieser Technologie können Datenbanken erstmals verschlüsselt genutzt werden. Auch eröffnen sich mit ihr zahlreiche neue Möglichkeiten im Bereich Multi-Cloud-Computing und Machine Learning. Zudem hat homomorphe Kryptografie politische Implikationen. Die Technologie ist zentral für die Sicherheitspolitik, etwa beim Datenaustausch zwischen Sicherheitsbehörden. Neue Multi-Cloud-Geschäftsmodelle könnten zudem neue Abhängigkeiten erzeugen, etwa von den USA, wo bereits an einer Standardisierung gearbeitet wird. Um nicht abgehängt zu werden, sollte die EU die Anwendungsforschung fördern und homomorphe Verschlüsselung bei den Planungen für die eigene Cloud-Initiative Gaia-X frühzeitig miteinbeziehen.

Verschlüsselung wandelt lesbaren Klartext mittels mathematischer Funktionen in unleserlichen Ciphertext um. Dadurch können nur autorisierte Nutzerinnen und Nutzer mit passendem Schlüssel eine Information dechiffrieren. Bisherige Verschlüsselungsverfahren haben aber einen zentralen Nachteil: Daten sind entweder im Klartext lesbar *oder* verschlüsselt. Wer Daten auf einer Festplatte bearbeiten will, muss diese zunächst entschlüsseln. Das erhöht das Risiko, dass unbefugte Dritte diese Daten mitlesen können. Datennutzung bei *gleichzeitiger* aktiver Verschlüsselung war lange Zeit praktisch kaum umsetzbar. Neue Entwicklungen im Bereich sogenannter vollständiger homomorpher Verschlüsselung (HV) lassen hoffen, dass dieses Problem gelöst werden kann. HV erlaubt die Nutzung von Daten in Datenbanken oder auf Festplatten, während sie noch verschlüsselt sind. Das ist gewissermaßen der »heilige Gral« der Verschlüsselung: Daten sind auf einmal zeitgleich nutzbar *und* sicher. Dank wissenschaftlicher Fortschritte und der Initiativen großer US-Firmen ist das mittlerweile nicht mehr nur eine Forschungstheorie, sondern wird zunehmend Praxis. HV wird ein zentraler Technologietrend in den nächsten Jahren sein, erlaubt sie doch komplett neue Anwendungsszenarien. Daher ist HV ein Schlüsselthema der IT-Sicherheit und der Technologiepolitik.

Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Was ist Homomorphe Verschlüsselung?

Homomorphe Verschlüsselung ist ein kryptografisches Verfahren, das insbesondere im Bereich der Datennutzung, etwa bei Datenbankabfragen oder beim Cloud-Computing, angewendet werden wird. Es ist also kein Verfahren für die Transportverschlüsselung, wie etwa bei Messenger-Kommunikation.

Homomorph heißt, dass Klartext und Ciphertext strukturtreu zueinander sind. Daher liefert die statistische Analyse homomorph verschlüsselter Daten ähnliche Resultate wie die von unverschlüsseltem Klartext. HV basiert auf bereits bekannten Public-Key-Verfahren der Transportverschlüsselung. Nur autorisierte Nutzerinnen und Nutzer können mit einem Mix aus privatem und öffentlichem Schlüssel Daten dechiffrieren. Allerdings erlaubt HV durch die Verwendung komplexer Algebra (u.a. »lattice-based« bzw. gitterbasierte Algebra) auch Berechnungen an verschlüsselten Daten. Damit können zum Beispiel verschlüsselte Datenbanken durchsucht werden, ohne dass diese entschlüsselt werden müssen.

Dr. Craig Gentry, einer der Vordenker von HV, beschreibt das Verfahren so: HV ist wie ein Handschuhkasten, mit dem toxische Materialien bearbeitet werden. Man kann die Hände in die Handschuhöffnungen stecken, ohne dass man notwendigerweise sieht, was man darin ergreift (ein Sinnbild für die Verschlüsselung). Man kann die Objekte innerhalb des undurchsichtigen Kastens greifen und mit ihnen »arbeiten« (Datenverarbeitung), aber es ist nicht möglich etwas aus dem Kasten herauszuholen.

Mit HV können Kunden also auf verschlüsselte Daten in einer Cloud zugreifen, ohne dass diese wie bisher an einer Stelle entschlüsselt werden und somit für den Cloud-Betreiber oder Dritte sichtbar werden. HV kann so gestaltet werden, dass bei Datenbankabfragen zum Beispiel die Eingaben und Ausgaben für Dritte verborgen bleiben, also für den Datenbankbetreiber selbst. Damit könnte nur ein Datenbanknutzer Eingaben und Ausgaben im Klartext sehen. Gleichzeitig kann eine homomorph verschlüsselte Datenbank sicherstellen, dass weitere Daten vor unbefugtem Zugriff der Nutzerinnen und Nutzer geschützt sind. Damit löst sich ein zentrales Datenschutzproblem, nämlich jenes des Misstrauens gegenüber Cloud-Diensten. Bisher kann man als Kunde nie sicher sein, was ein Cloud-Anbieter mit dort gespeicherten Daten anstellt. HV erlaubt also eine ähnliche Funktionalität, wie sie unverschlüsselte Datenbanken haben, bei gleichzeitig besserer Datensicherheit.

Die genaue Funktionalität hängt aber von dem verwendeten Verfahren ab. Es gibt partielle, einigermaßen vollständige und vollständige homomorphe Kryptografie. Die verschiedenen Systeme erlauben unterschiedliche Arten von Berechnungen an verschlüsselten Daten und haben teils eigene Limitierungen, etwa bei der Anzahl der Abfragen. Der Grad der Datensicherheit ist also eine Frage der Implementierung des gewählten Verfahrens.

Anwendungsszenarien

Die Nutzungsszenarien sind vielfältig. Ein großer Bereich, in dem HV voraussichtlich eine starke Rolle spielen wird, ist Datenbank-Outsourcing. HV-verschlüsselte Datenbanken können an Dritte outgesourct werden, ohne dass diese die Datenbankinhalte lesen können. Dennoch können natürlich Berechnungen damit durchgeführt werden. Durch diese Möglichkeit des Outsourcings eröffnen sich vollkommen neue Geschäftsmodelle. So könnten medizinische Datenbanken zur weiteren statistischen Analyse an Dritte weitergegeben werden, ohne dass individuelle Datenpunkte einzelnen Patienten zugeordnet werden können. Damit sind medizinische Studien mit kombinierten Datenbanken machbar, ohne dass die Privatsphäre Einzelner verletzt wird. Die Kombination verschiedener Cloud-Datenbanken, auch Multi-Cloud-Computing genannt, ist ein Trend der kommenden Jahre. Bisher sind damit enorme logistische Herausforderungen verknüpft, die durch die Schwierigkeit

entstehen, Daten über verschiedene Datenbanken hinweg sicher zu verschlüsseln.

Das Kombinieren diverser Datenbanken ist auch in der Sicherheitspolitik relevant. HV kann Probleme beim Datenaustausch zwischen Datenbanken verschiedener Sicherheitsbehörden lösen. Mit HV können einzelne Datenpunkte geteilt werden, ohne dass die Gefahr eines unbefugten Zugriffs Dritter auf die gesamte Datenbank besteht. Ein solcher Austausch ist nämlich bisher sowohl bei Fahndungsdatenbanken als auch beim »intelligence sharing« zwischen Nachrichtendiensten ein Problem, was dazu führt, dass darauf verzichtet wird. Auch bei vernetzten militärischen Einsatzführungssystemen kann HV sinnvoll sein. Standardmäßig mit HV verschlüsselte Datenbanken wären auch in der IT-Sicherheit ein äußerst wirkungsvolles Mittel gegen die zunehmenden Datenlecks. Auch bei der Digitalisierung demokratischer Prozesse kann HV helfen. Microsoft hat jüngst sein »Election Guard«-Programm vorgestellt. Damit können über elektronische Wahlgeräte abgegebene Wahlstimmen verifiziert und von Wahlleitern aggregiert werden, ohne dass die individuelle Wahlpräferenz offengelegt wird. HV ist also eine wichtige Technologie für den Schutz der Privatsphäre. Der größte Nutzen dürfte im Bereich Machine Learning (ML) und Künstliche Intelligenz liegen. Mittels HV können ML-Algorithmen Analysen an Datensätzen ausführen, ohne das Trainingsmodell oder einzelne Datenpunkte offenlegen zu müssen und damit die Privatsphäre einzelner Nutzerinnen und Nutzer zu gefährden.

Wo stehen wir?

Die Ursprünge von HV reichen bis in die 1970er Jahre zurück. 2009 veröffentlichte Craig Gentry eine Promotion zum Thema, die als Meilenstein gilt. Der Nachteil an Gentrys Verfahren war bis vor kurzem die unpraktische Umsetzbarkeit. Die Berechnungen an verschlüsselten Datenbanken sind bisher noch langsamer als die an Klartext. Die IT-Firma IBM schätzt, dass Berechnungen via HV bisher noch zehn- bis hundertmal mehr Rechenleistung benötigen als unter Einsatz anderer Kryptoverfahren. Zudem erhöht sich der Speicherverbrauch je nach Verfahren um den Faktor 20. Für Berechnungen an komplexen neuronalen Netzen oder für Echtzeitberechnungen ist das noch unpraktikabel. Zudem sind HV-Algorithmen bisher aufwendig in der Implementierung und umständlich in der Nutzbarkeit.

Allerdings wurden seit 2009 enorme Fortschritte gemacht. Algorithmen wurden verbessert und die Rechenleistung stieg an, so dass diese in Zukunft immer weniger ein limitierender Faktor sein werden. Da HV der nächste logische Entwicklungsschritt nach Cloud-Computing, Big Data, dem Internet der Dinge und Machine Learning ist, wird die Optimierung von HV durch diese Trends befeuert. Dadurch wird sich auch mittelfristig die Nutzbarkeit verbessern und auch die Verbreitung erhöhen.

Das liegt auch daran, dass sich mehrere große Player das Thema auf die Fahne geschrieben haben. Die US Defense Advanced Research Projects Agency investiert schon seit 2011 in die Technik. Das DPRIVE-Programm zielt darauf, HV-Algorithmen zu beschleunigen und die Rechenintensität zu reduzieren.

Microsoft gab 2015 das Projekt SEAL als Open Source frei. SEAL ist eine vollständige Programmbibliothek, die Nutzerinnen und Nutzern HV ermöglicht, ohne komplexe mathematische Modelle zu benötigen.

In die gleiche Kerbe schlägt auch IBM mit seinem 2020 gestarteten HElib-Projekt. Dabei handelt es sich um einen HV-Werkzeugkasten samt Testumgebung, mit dem User zum Beispiel eigene Prototyp-Anwendungen erstellen können.

Weitere Player sind die U.S. National Security Agency und kleinere Startups in den USA, unter anderem Enveil. Zudem werden in der Wissenschaft zahlreiche weitere Varianten und Toolkits entwickelt, um die oben genannten Probleme zu überwinden. Auch in China werden zunehmend Forschungspapiere zum Thema HV veröffentlicht. In Deutschland und Europa

steckt die Entwicklung noch in den Kinderschuhen. SAP, die Fraunhofer-Institute und verschiedene universitäre Projekte arbeiten vorwiegend an den theoretischen Aspekten der Technologie.

Die wissenschaftlichen Erkenntnisse in die Praxis umzusetzen, etwa um neue Geschäftsfelder frühzeitig zu besetzen, gestaltet sich in der EU allerdings schwieriger als in den USA. Das 2015 gestartete HEAT-Projekt der EU soll das ändern. Experten und Expertinnen schätzen, dass in ungefähr fünf Jahren die Anwendungsreife dieser Technologie erreicht ist. Ungefähr in dieser Zeitspanne werden auch Multi-Cloud-Architekturen zum Standard werden. Es ist also wichtig, dieses Thema jetzt schon auf dem Schirm zu haben.

Implikationen für die digitale Souveränität Europas

Die groben Umrisse der politischen Implikationen dieser Technologie sind heute schon sichtbar. Erstens wird die Einführung von HV ähnliche Auswirkungen haben wie die anderer Verschlüsselungsmethoden: Sicherheitsbehörden werden versuchen, die Technik zu schwächen, da sie im Widerspruch zu ihren Überwachungsbemühungen steht. Hintertüren in Standard-Software sind zu befürchten. Da HV auf Public-Key-Verfahren aufsetzt, ergäben sich ähnliche Grundprobleme. Die Sicherheit von HV hängt von der Implementierung und der Sicherheit des Gesamtsystems ab. Softwareschwachstellen, ob intentional platziert oder zufällig, können auch hier die IT-Sicherheit gefährden. Auch das komplexe Schlüsselhandling kann schiefgehen und ein Einfallstor öffnen.

Daraus ergeben sich, zweitens, Fragen für das Spannungsfeld digitaler Autonomie und Abhängigkeit Europas von US-Technologie. Diverse wissenschaftliche Arbeitsgruppen und Unternehmen wie Microsoft und IBM arbeiten zusammen mit dem U.S. National Institute of Standards and Technology (NIST) bereits an der Standardisierung homomorpher Verfahren. Zwar hätte ein NIST-Standard für HV keine bindende, durchaus aber eine Signalwirkung für Europa. Wer auch immer den Entwicklungsschritt zu praktikabler HV frühzeitig meistert, hat einen Vorteil bei der nächsten Generation der Kryptografie. In der Theorie ist es möglich, mit vollständig homomorphen Verfahren quantensichere Verschlüsselung herzustellen. Quantencomputer können kryptografische Verfahren, die bisher als sicher galten, brechen. Vollständige HV bietet in der Theorie einen Schutz davor. Das heißt, der, dem die praktische Umsetzung dieser Technologie als Erstem gelingt, hat einen Startvorteil im bevorstehenden Quantenzeitalter.

Jetzt ist noch Zeit, um auf diese Entwicklungen zu reagieren. So sollte die EU die Standardisierung beschleunigen. Die Standardisierung von HV für Multi-Cloud-Umgebungen ist wichtig, damit Daten zwischen Anbietern sicher ausgetauscht werden können. So kann ein »vendor lock-in« — die Abhängigkeit von amerikanischen Services — frühzeitig vermieden werden.

Um die eigene digitale Souveränität zu stärken, sollte die EU der Wissenschaft und Startups mehr Finanzmittel für die Anwendungsforschung über HV bereitstellen. Denn aus der Anwendungsforschung lassen sich frühzeitig die Geschäftsmodelle der Zukunft entwickeln. Diese sollten auch durch Venture-Kapital gefördert werden. Datensparsame Cloud-Services, die das grundsätzliche Misstrauensproblem lösen, stellen eine konkrete Marktlücke dar. Vertrauenswürdige europäische Cloud-Services können ein Wettbewerbsvorteil gegenüber chinesischen oder amerikanischen Services sein, die im Bereich Cloud-Computing marktführend sind. Mittels HV könnte auch die von Deutschland und Frankreich initiierte Prestige-Cloud-Plattform Gaia-X aufgewertet werden. Bei deren Aufbau sollte HV von Anfang an mitgedacht werden. Bei HV hat Europa die Gelegenheit auf einen Zug aufzuspringen, der zwar bereits rollt, aber noch nicht vollständig abgefahren ist.

Dr. Matthias Schulze ist Stellvertretender Leiter der Forschungsgruppe Sicherheitspolitik.

Der Autor dankt Prof. Lena Wiese und Dr. Michael Brenner für Ideen und Feedback.

SWP
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Ludwigkirchplatz 3—4
10719 Berlin
Telefon +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN (Print) 1611-6364
ISSN (Online) 2747-5018
doi: 10.18449/2021A15