idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Pressemitteilung

Hochschule Darmstadt
Simon Colin

19.10.2021
http://idw-online.de/de/news777744

Forschungsprojekte
Informationstechnik
überregional

Schutz vor Quantencomputern: Experten der h_da wollen bestehende IT-Systeme sicherer machen

Kommt der leistungsfähige Quantencomputer, wäre das Internet, wie wir es heute kennen, nicht mehr sicher. Derzeit übliche, so genannte Public-Key-Verschlüsselungsverfahren haben dann keinen Bestand mehr. Forscher vom Fachbereich Informatik der Hochschule Darmstadt (h_da) befassen sich mit Post-Quanten-Kryptografie und damit, wie sich existierende IT-Architekturen auf Quantencomputer-resistente Verschlüsselungsverfahren umstellen lassen. Ihr Projekt „Agile and Easy-to-Use Integration of PQC Schemes“ ist Teil des Nationalen Forschungszentrums für angewandte Cybersicherheit ATHENE.

Für die Dauer von vier Jahren wird es mit rund 560.000 Euro gemeinsam vom Bundesministerium für Bildung und Forschung und vom Hessischem Ministerium für Wissenschaft und Kunst gefördert.

Digitale Sicherheit im Internet beruht derzeit weitgehend auf so genannter Public-Key-Kryptografie. Hier verfügt jeder Nutzer und jede Nutzerin beim Mailen, Chatten oder Online-Einkauf über ein sicheres Schlüsselpaar: Einen öffentlichen Key, mit dem Daten verschlüsselt werden, und einen privaten Key, mit dem beim rechtmäßigen Empfänger die Daten entschlüsselt werden. Mit heutigen Mitteln sind die gängigen Public-Key-Verfahren nicht zu brechen.

„Der Quantencomputer jedoch ändert alles“, sagt Prof. Dr. Andreas Heinemann. “Einem solch leistungsstarken Rechner genügt der öffentliche Schlüssel, um den privaten zu bestimmen. Um mit dem Faktor Zeit zu sprechen, würde das bedeuten: Braucht ein konventioneller Computer Millionen Jahre, um alle Bestandteile und Variationsmöglichkeiten des Schlüssels auszurechnen, schafft ein Quantencomputer das in wenigen Stunden oder Tagen. Das ist eine fundamentale Bedrohung der IT-Sicherheit."

Prof. Dr. Andreas Heinemann und sein Kollege Prof. Dr. Alexander Wiesmaier arbeiten daran, hierauf vorbereitet zu sein. Nach bisherigen Erkenntnissen ist zwar noch kein leistungsfähiger Quantencomputer weltweit verfügbar, der die gängigen Public-Key-Krypto-Verfahren brechen könnte, aber für die Professoren für IT-Sicherheit lautet die Frage schon lange nicht mehr ob, sondern nur noch, wann es ihn geben wird. „Dann ist alles mit einem Schlag unsicher, was wir bisher im Internet machen“, ordnet Andreas Heinemann ein. „Der Online-Einkauf, Urlaubs- oder Ticketbuchungen, Online-Bezahldienste, die Steuerabgabe, E-Mails oder das Chatten in den Sozialen Medien, eben jegliche Kommunikation, deren Sicherheit und Privatheit auf mit Public-Key-Kryptografie verschlüsselten Daten basiert.“

Die h_da-Forschenden wollen mit ihrer Arbeit dazu beitragen, dass die bestehende Infrastruktur, heutige Computer samt Software, auch weiterhin benutzt werden kann, nur eben mit neuen, Quantencomputer-resistenten Verschlüsselungen. In der Post-Quanten-Kryptografie geht es genau darum: Nutzerinnen und Nutzer herkömmlicher IT-Architektur vor Angriffen zu schützen, die einen Quantencomputer verwenden.

Das h_da-Vorhaben ist eines von drei Projekten im Forschungsbereich Kryptografie beim Nationalen Forschungszentrum für angewandte Cybersicherheit ATHENE in Darmstadt. Während die anderen beiden Kryptografie-Projekte des ATHENE Zentrums an der Analyse, Entwicklung und Implementierung neuer Sicherheits-Algorithmen zur Verschlüsselung forschen, befasst sich das h_da-Team mit der Frage, wie diese neuen Verfahren – an denen bereits gearbeitet wird – künftig leicht und leistungsfähig in heutige IT-Systeme integriert werden können. „Wir bewerten die praktische Umsetzbarkeit neuer möglicher Sicherheits-Algorithmen in bestehende Software-Produkte“, erläutert Alexander Wiesmaier den Forschungsfokus.

Bislang verursacht die Migration, der Wechsel von den klassischen zu Post-Quanten-Verschlüsselungsverfahren, Probleme. Die vorhandene Infrastruktur kann nicht von heute auf morgen umgestellt werden. „Ich kann nicht einfach meinen Online-Shop, meinen Service oder meine Produktion wochenlang schließen. Es wird eine Übergangszeit geben, für die wir Lösungen suchen müssen, damit Geräte mit unterschiedlicher Kryptografie sich noch verstehen“, sagt Alexander Wiesmaier.

Erst langsam kommt das Thema auch in der Praxis, im Mittelstand und in der Industrie an. „Die meisten können mit dem Begriff Post-Quanten-Kryptografie noch nichts anfangen“, so Heinemann. IT-Sicherheit, weiß sein Kollege Wiesmaier, ist für Betriebe, den Handel und Unternehmen nicht nur ein technischer, sondern auch ein monetärer Faktor. „Oftmals wird die Sicherheit auf ein kostengünstiges Maß heruntergeschraubt. Langfristig werden aber alle auf Post-Quanten-Kryptografie umstellen müssen.“

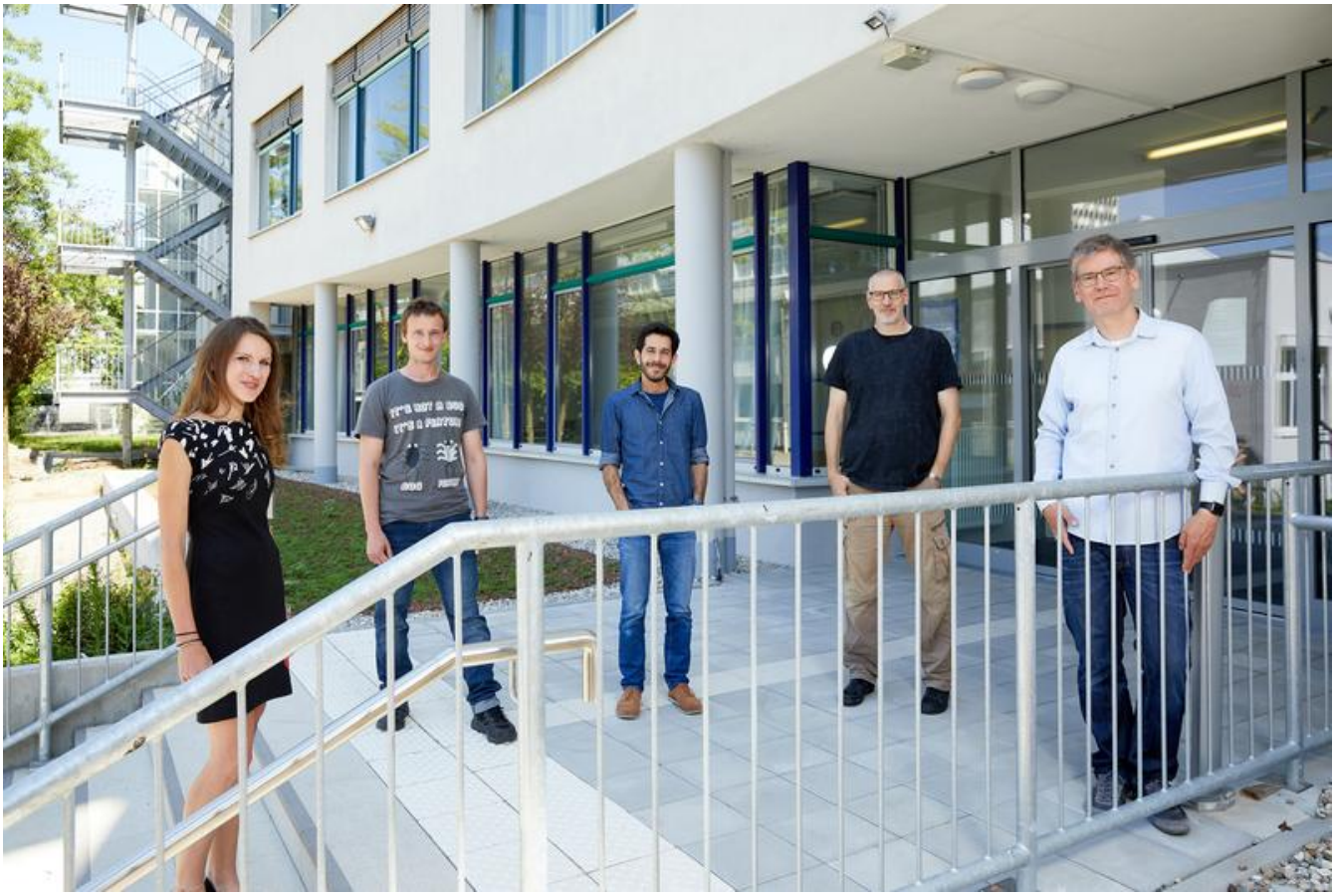
Dem h_da-Team ist daran gelegen, für ihre Forschung das Wissen möglichst vieler Wissenschaftlerinnen und Wissenschaftler zu nutzen. Sie haben eine Community-Webseite zum Thema Migration und Agilty von Post-Quanten-Kryptoverfahren eingerichtet, die für alle zugänglich ist. Es soll ein Sammelbecken sein für alle, die am Thema forschen. „Ein gemeinsamer Wissenstopf zum Nutzen aller“, betont Alexander Wiesmaier, „jede und jeder ist eingeladen, sich dort umzusehen oder aktiv zu beteiligen“.

Projekt-Website: https://fbi.h-da.de/pqc
Link zur Community-Webseite: https://fbi.h-da.de/cma

wissenschaftliche Ansprechpartner:

Ansprechpartner für die Medien
Hochschule Darmstadt
Fachbereich Informatik

Prof. Dr. Andreas Heinemann
Tel.: 06151-16-38482
E-Mail: andreas.heinemann@h-da.de



Prof. Dr. Andreas Heinemann und Prof. Dr. Alexander Wiesmaier mit ihren Doktoranden Nouri Alnahawi und Nicolai Schmitt sowie Master-Studentin Johanna Henrich (von rechts). Sie arbeiten an Verschlüsselungen, die Quantencomputern standhalten können.
Britta Hüning
h_da/Britta Hüning