idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

## Press release

### Fraunhofer-Institut für Sichere Informationstechnologie SIT
### Oliver Küch

03/20/2018
http://idw-online.de/en/news691158

Research results, Transfer of Science or Research
Economics / business administration, Information technology, Mathematics, Politics, Social studies
transregional, national

# Next Generation Cryptography

**Experten warnen: Kryptografie muss dringend flexibler werden, um schnell auf technische Veränderungen reagieren zu können. Falls dies nicht umgehend geschieht, droht der Cyberwelt ein Supergau. Das ist das Ergebnis des Eberbacher Gesprächs zu "Next Generation Cryptography", bei dem Experten aus Wirtschaft, Wissenschaft und Politik die Zukunft der Kryptografie diskutierten. Der vollständige Ergebnisbericht ist jetzt kostenlos auf der Internetseite des Fraunhofer-Instituts für Sichere Informationstechnologie SIT erhältlich.**

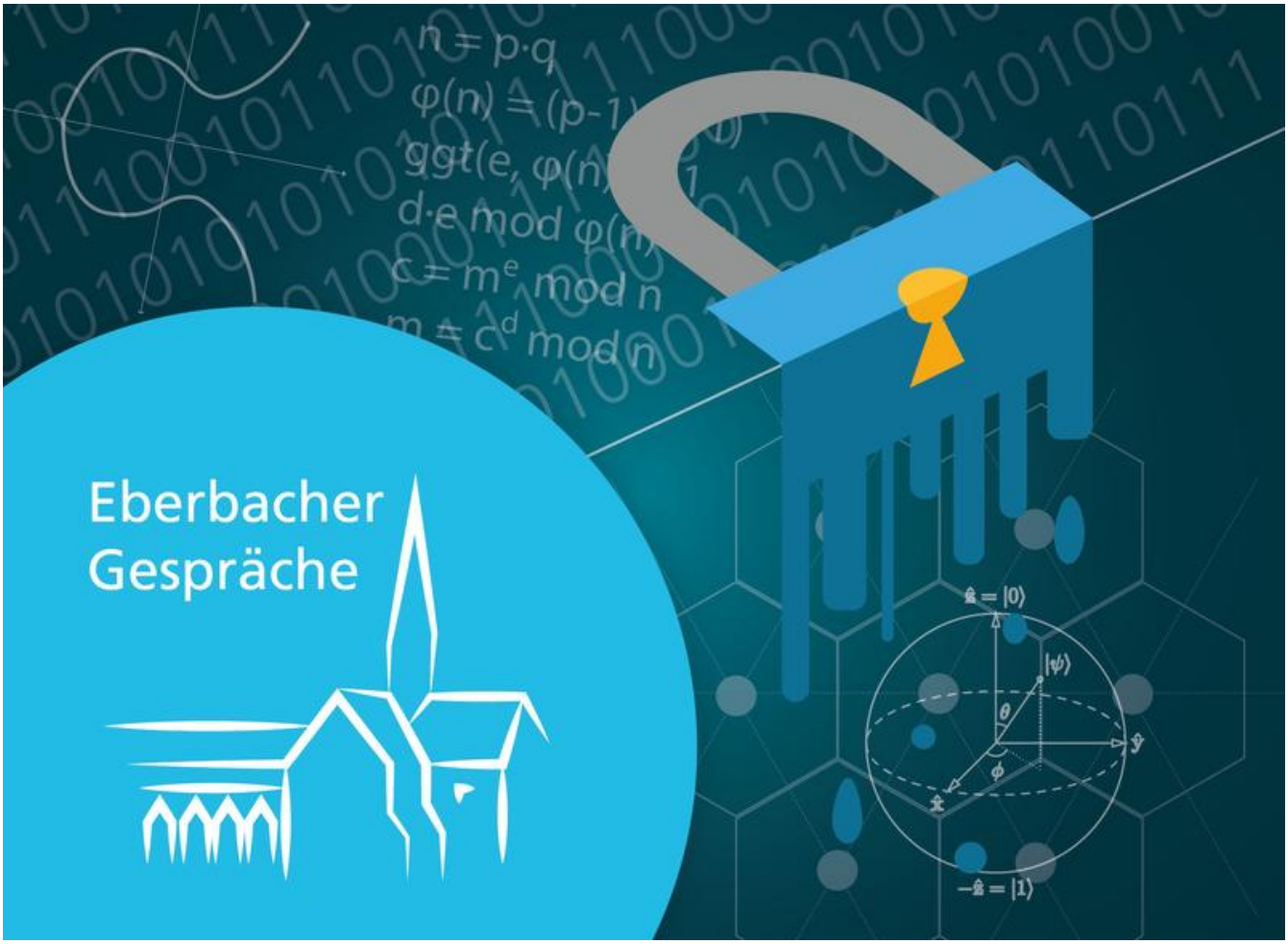
Ob Online-Banking oder Blockchain – die meisten IT-Sicherheitsmechanismen für Daten und digitale Kommunikation¬ beruhen auf Kryptografie. Quantencomputer und neue Angriffsmöglichkeiten bedrohen zahlreiche dieser IT-Sicherheitsmechanismen. Wie Wirtschaft und Gesellschaft die Cyberwelt in der Zukunft vor solch großen Bedrohungen schützen können, diskutierten Experten aus Wirtschaft, Forschung und Politik beim Eberbacher Gespräch „Next Generation Cryptography“. Das Fazit der Experten: Kryptografie muss dringend flexibler werden, um schnell auf technische Veränderungen reagieren zu können. Falls dies nicht umgehend geschieht, droht der Cyberwelt ein Supergau. Die Experten empfehlen deshalb Aufklärung, die Entwicklung von Praxishilfen sowie EU-Mindeststandards und einen EU-Expertenrat für Kryptografie. Der vollständige Bericht ist im Internet unter www.sit.fraunhofer.de/eberbach-crypto kostenlos verfügbar.

In der heutigen digitalisierten und vernetzten Welt sehen sich Unternehmen und Privatpersonen, Politik und Gesellschaft täglich mit Herausforderungen durch Sicherheitslücken und Bedrohungen durch IT-Angriffe konfrontiert. Die Industrie liefert sich ein Wettrüsten mit Angreifern, die versuchen, kryptografische Schlüssel, Protokolle oder Implementierungen zu brechen. Systeme, die Kryptografie beispielsweise für Verschlüsselung und digitale Unterschriften nutzen, müssen deshalb ständig nachgerüstet und verbessert werden, um aktuellen Angriffen standhalten zu können. Heute weit verbreitete kryptografische Verfahren sind zudem einer ständigen Erosion ausgesetzt: Die Steigerung der Rechenleistung potenzieller Angreifer erzwingt eine regelmäßige Anpassung und Erhöhung von Schlüssel-Längen und Sicherheitsparametern. Zudem müssen veraltete Verfahren und Protokolle ersetzt werden, und in Extremfällen könnten einzelne kryptografische Verfahren über Nacht unsicher werden.

Dieser andauernde Wettlauf wird durch die Entwicklung von Quantencomputern entscheidend beeinflusst werden. Im Vergleich zu klassischen Computern werden Quantencomputer die erforderliche Zeit für Angriffe auf kryptografische Verfahren extrem verkürzen können. Bislang sind Quantencomputer vorwiegend ein Forschungsobjekt und die ersten kommerziellen Prototypen stellen noch keine Bedrohung für die heutige Kryptografie dar. Doch China und andere Länder investieren massiv in die Entwicklung von Quantencomputern, sodass es nur eine Frage der Zeit ist, bis ein ausreichend mächtiger Quantencomputer die heutige Kryptografie dramatisch verändern wird. Angreifer werden mit Hilfe eines Quantencomputers nicht nur einzelne Services oder Produkte unbrauchbar machen, sondern ganze kryptografische Algorithmen wie RSA, DSA, DH und ECC aushebeln können. Damit sind beispielsweise sämtliche Daten und digitale Unterschriften, die mit diesen Algorithmen geschützt werden, sofort unsicher – die Auswirkungen betreffen nicht nur einzelne Unternehmen, sondern große Teile von Wirtschaft und Gesellschaft.

Das Fraunhofer SIT hat IT-Sicherheitsexperten aus Wirtschaft und Wissenschaft zu einem Eberbacher Gespräch über „Next Generation Cryptography“ eingeladen, um die kommenden Herausforderungen für IT-Sicherheitstechnologien zu diskutieren. Die Teilnehmer des Eberbacher Gesprächs haben sieben Empfehlungen an Wirtschaft und Politik ausgesprochen. Die Experten empfehlen, Mindeststandards für IT-Sicherheitslösungen in Wirtschaft und Industrie zu entwickeln, um mehr Business-IT-Sicherheit zu gewährleisten. Darüber hinaus soll ein „Handbuch für Kryptografie-Lösungen“ dabei helfen, schneller und leichter sichere IT-Produkte zu entwickeln. Die USA sind bereits dabei, alternative kryptografische Verfahren zu standardisieren. Deshalb appellieren die Experten an EU-Entscheidungsträger, rechtzeitig in die Entwicklung neuer Kryptografie-Alternativen zu investieren und die Förderung von agiler Kryptografie strategisch anzugehen, um die zukünftige technologische Weltkarte aktiv mitzugestalten. Eine Empfehlung der Experten: Auch die Europäische Union sollte Standards für Kryptografie entwickeln. Zudem soll ein Rat von Krypto-Weisen ins Leben gerufen werden, der Empfehlungen entwickelt und politische Vertreter in Fragen zu Entwicklung und Standardisierung beraten kann. Darüber hinaus soll die breite Öffentlichkeit für IT-Sicherheitsfragen sensibilisiert und in Kryptografie ausgebildet werden.
Das vollständige Papier ist jetzt veröffentlicht worden und kann hier kostenlos heruntergeladen werden: www.sit.fraunhofer.de/eberbach-crypto.

Attachment Eberbacher Gespräch - Abschlussbericht http://idw-online.de/en/attachment65039




Quantencomputer und neue Angriffsmöglichkeiten bedrohen aktuelle IT-Sicherheitsmechanismen. Experten sehen dringenden Handlungsbedarf.

Fraunhofer SIT