Westfälische
Wilhelms-Universität
Münster

FACHBEREICH 10
MATHEMATIK UND INFORMATIK
Prof. Dr. Martin Stein
Dekan

08.01.2013

Einladung

Am Montag, 28.01.2013, 16:30 Uhr, Hörsaal M6

spricht

Prof. Dr. Frederik Armknecht

über

"Homomorphe Verschlüsselungsverfahren"

Das Konzept des Cloud-Computings stellt eines der wichtigsten Paradigmenwechsel in der heutigen IT-Welt dar. Datenspeicherung und Berechnungen finden nicht mehr lokal statt, sondern werden über entsprechende Dienste ausgelagert. Allerdings birgt dieser Ansatz das große Risiko des Datenmissbrauchs in sich, etwa durch Sicherheitslecks oder gar bösen Absichten bei dem Cloud-Anbieter. Eine zentrale Herausforderung, die für eine weitere Akzeptanz des Cloud Computings gelöst werden muss, ist daher die folgende: Wie kann man Daten und Berechnungen sicher auslagern, ohne dem Anbieter zwangsläufig vertrauen zu müssen?

Man überlegt sich leicht, dass wenn keinerlei Vertrauen zu den involvierten Service-Anbietern besteht, die Daten einerseits intrinsisch gegen unerlaubtes Auslesen geschützt sein müssen, andererseits der Service Provider nach wie vor in der Lage sein sollte, erwünschte Berechnungen auf diesen Daten durchzuführen. Für diese zunächst widersprüchlichen Anforderungen bietet die moderne Kryptographie einen vielversprechenden Lösungsansatz: homomorphe Verschlüsselungsverfahren. Hierbei werden Daten in einer Art und Weise verschlüsselt, die es erlaubt, anstelle von Berechnungen auf den Klartexten durchzuführen, entsprechende Operationen auf den verschlüsselten Daten anzuwenden. Das Ergebnis ist dann eine Verschlüsselung des Berechnungsergebnisses. Ein Benutzer könnte somit seine verschlüsselten Daten auslagern, auf denen der Service-Provider auf Anfrage entsprechende Operationen durchführt, ohne dass dieser etwas über den Inhalt der Daten oder dem Ergebnis der Berechnungen erfährt.

In diesem Vortrag werden nach einer Einführung in die Thematik der homomorphen Verschlüsselungsverfahren einige aktuelle Ergebnisse beschrieben und zukünftige Forschungsrichtungen aufgezeigt.

Auf diesen Vortrag wird besonders hingewiesen

Martin Stein, Dekan