ROUTE

Cryptography for the Post-Quantum Era

Programm / Ausschreibung	KIRAS, F&E-Dienstleistungen, KIRAS F&E-Dienstleistungen 2019	**Status**	abgeschlossen
Projektstart	01.10.2020	**Projektende**	30.09.2021
Zeitraum	2020 - 2021	**Projektlaufzeit**	12 Monate
Keywords	asymmetrische Kryptographie; Verschlüsselung; Schlüsselaustausch; Signaturen		

Projektbeschreibung

Staatliche Einrichtungen sind zunehmend das Ziel von großangelegten Cyberattacken. Bei diesen Angriffen besteht die Gefahr, dass schützenswerte Daten den Angreifern in die Hände fallen. Um den rechtlichen Grundlagen zur langfristigen Informationssicherheit gerecht zu werden, ist deshalb die Koordination von Richtlinien für sichere Informationssystemen eine der Kernaufgaben der Bedarfsträger. Kryptographische Verfahren bieten in diesem Fall die Möglichkeiten die Vertraulichkeit von Daten zu gewährleisten solange das entsprechende Schlüsselmaterial geheim bleibt. Jedoch sind die Sicherheitsgarantieren für die aktuell genutzten Verfahren durch Angreifer mit Zugang zu Quantencomputern gefährdet. Leistungsfähige Quantencomputer wären in der Lage große Teile der heute verwendeten asymmetrische Kryptographie (asymmetrische Verschlüsselung, Schlüsselaustausch, digitale Signaturen) effizient zu brechen. Damit wäre die sichere Speicherung („data at rest“) mittels asymmetrischer Verschlüsselung nicht mehr gegeben. Auch die sichere Kommunikation solcher Daten („data in transit“), die mittels Schlüsselaustauschverfahren die Vertraulichkeit und digitalen Signaturverfahren die Authentizität der Daten bzw. die Identitäten der kommunizierenden Parteien sicherstellen, wären von dieser Gefahr betroffen.

Um diesem Bedrohungsszenario vorzubeugen und die Grundlage für einen raschen Umstieg auf quanten-resistente Kryptographie zu ermöglichen, analysiert das Projekt ROUTE den Stand der Technik kryptographischer Verfahren für klassische Computer, die auf quanten-resistenten mathematischen Problemen basieren - so genannter Post-Quanten-Kryptographie - und deren Sicherheit auch durch leistungsfähige Quantencomputer nicht bedroht wird. Als Ziel des Projekts werden Empfehlung zum Einsatz ausgewählter post-quanten-sicheren Verfahren erarbeitet. Zwar werden inzwischen erste Bemühungen unternommen Post-Quanten-Kryptographie zu standardisieren und von der Industrie vereinzelt in Produkten getestet, jedoch stellt sich dabei heraus, dass die vorgeschlagenen Verfahren nicht uneingeschränkt für alle Anwendungsszenarien geeignet sind. Deshalb werden in ROUTE die Empfehlung basierend auf den Sicherheitsgarantieren und abgestimmt auf die Anwendungen „data at rest“ und „data in transit“ getroffen. Dazu werden die Verfahren (1) anhand der Konfidenz in die darunter liegenden Annahmen und der Konstruktionsstrategie analysiert, (2) die Effizienz der Verfahren empirisch erhoben und (3) die verfügbaren Implementierungen hinsichtlich ihrer Qualität und Sicherheit untersucht.

Abstract

Government facilities are targeted more and more by large-scale cyber-attacks. During such attacks, the attackers might gain access to sensitive data. Yet, the public institutions are obliged by law to ensure the confidentiality of the data by coordinating recommendations for secure information systems. To protect data from such attacks, cryptographic schemes can be employed to ensure the data's confidentiality, integrity and authenticity as long as the secret key material stays secret. However, the schemes used in practice today are threatened by quantum computers. Powerful quantum computers would be capable of breaking essentially all asymmetric cryptographic schemes (public-key encryption, key encapsulation, and digital signatures). Consequently, the security of long-term storage of confidential data ("data at rest") ensured by using public-key encryption would be compromised. Similarly, protocols for securely transmitting data ("data in transit") using key encapsulation methods to ensure confidentiality and digital signatures to ensure authenticity of data and the communicating parties would be compromised as well.

To mitigate this attack scenario and to prepare for a switch to quantum-resistant cryptography, the project ROUTE analyzes the state of the art of cryptographic schemes that are based on quantum-resistant problems – classified as post-quantum cryptography – which are not threatened by powerful quantum computers and will provide recommendations for the deployment of post-quantum secure schemes. Although first standardization efforts for post-quantum cryptography are being carried out and industry is integrating schemes in products for testing, it turns out that the selection of suitable schemes is more complicated. They are no longer suitable for all possible use-cases. Therefore, ROUTE will match the recommendations with the requirements of the usage scenarios "data at rest" and "data in transit" and their security properties. To achieve that, ROUTE evaluates the schemes based on (1) the security analysis of the underlying hardness assumptions and of the concrete constructions, (2) their efficiency which is being evaluated empirically, and (3) quality and security of the available implementations.

Projektkoordinator

- AIT Austrian Institute of Technology GmbH

Projektpartner

- Bundesministerium für Inneres
- Bundeskanzleramt