Kryptovergleich

Vergleich von physikalischen Methoden zur quantencomputersicheren Erzeugung und Verteilung kryptografischer Schlüssel

Programm / Ausschreibung	KIRAS, F&E-Dienstleistungen, KIRAS-Kybernet-Pass CS F&E Dienstleistungen (CS FED_2023)	**Status**	laufend
Projektstart	01.10.2024	**Projektende**	23.12.2025
Zeitraum	2024 - 2025	**Projektlaufzeit**	15 Monate
Keywords	Kryptografie, Quantencomputer, Schlüsselverteilung		

Projektbeschreibung

Die Digitalisierung, Globalisierung und Vernetzung benötigen eine sichere Telekommunikation und diese wiederum erfordert eine sichere Kryptographie. Mit dem Erscheinen von leistungsfähigen Quantencomputern in der Zukunft ist die heutige asymmetrische Kryptografie aus Sicherheitsgründen nicht mehr verwendbar, was schon heute für gewisse Daten relevant ist. Daher wird schon seit Jahrzehnten versucht physikalische Verfahren der Kryptografie zu finden, insbesondere zur Erzeugung und Verteilung kryptografischer Schlüssel.
Die Studie analysiert und vergleicht technologieneutral, allgemein verständlich und nachvollziehbar vier verschiedene Methoden von physikalischen Verfahren der Kryptografie inklusive der dahinterliegenden verschiedenen Technologien und der verfügbaren und geplanten kommerziellen Produkte / Lösungen. Die vier Methoden sind QKD (Quantum Key Distribution) mit und ohne Verschränkung, Verfahren, die auf der Messung von Funkkanaleigenschaften basieren, und Schlüsselverteilung durch hochsichere SSD/HDD/Memory Stick. Bei den ersten drei Methoden wird unterschieden zwischen einer Realisierung über Glasfasernetze, Freistrahlkanäle und Satellitenverbindungen.
Die Ergebnisse der Studie sind ein umfangreicher Vergleich aus der Sicht der IT-Sicherheit, Funktionalität, Marktreife, Schlüsselrate und Kosten. Des Weiteren erfolgt eine technologieneutrale Analyse der Vor- und Nachteile und der generellen Eignung der vier Methoden und Produkte/Lösungen in Bezug auf verschiedene Anwendungsszenarien.
Die Studie wird von IT-Sicherheitsexperten vor allem für Beschaffer*innen (Einkäufer*innen), Sicherheitsverantwortliche und Anwender*innen verfasst.
Es existieren heute schon viele verschiedene geeignete Technologien und Produkte / Lösungen am Markt, die meist technologienahe beschrieben sind. Sie stellen heute für Beschaffer*innen, IT-Sicherheitsverantwortliche und Anwender*innen ein undurchsichtiges Konvolut dar, die noch in keiner Studie in Bezug auf IT-Sicherheit, Marktreife, Kosten, Anwendbarkeit etc. technologieneutral und allgemein verständlich analysiert und vergleichen wurden.

Abstract

Digitalization, globalization and networking require secure telecommunications, which in turn require secure cryptography. With the advent of suitable quantum computers in future, today's asymmetric cryptography can no longer be used for security reasons, which is already relevant for certain data. For this reason, attempts have been made for decades to find

physical methods of cryptography, in particular for the generation and distribution of cryptographic keys.
The study analyzes and compares four different methods of physical cryptography, including the underlying technologies and the available and planned commercial products / solutions, in a completely technology-neutral, understandable and comprehensible manner. The four methods are QKD (Quantum Key Distribution) with and without entanglement, methods based on the measurement of radio channel properties and key distribution using highly secure SSD/HDD/memory sticks. A distinction is made between implementation via fiber optic networks, free beam channels and satellite connections
The results of the study are a comprehensive comparison from the point of view of IT security, functionality, market maturity, key rate and costs. Furthermore, a technology-neutral analysis of the advantages and disadvantages and general suitability of the four methods and commercial products / solutions in relation to different application scenarios is carried out.
The study is written by IT security experts primarily for procurers, security managers and users.
There are already many different suitable technologies and, above all, products/solutions on the market today, most of which are described in very technological terms. For procurers, IT security managers and users, they represent an opaque convolute that has not yet been analyzed and compared in any study in terms of IT security, market maturity, costs, applicability etc. in a technology-neutral and generally understandable way.

Endberichtkurzfassung

Die Studie ist vor allem interessant für Leser, die in ihrem Umfeld eine sehr hohe Datensicherheit benötigen bzw. die sich für sehr hohe Datensicherheit und/oder Kryptografie interessieren. Sie behandelt allgemein verständlich drei QKD (Quantum Key Distribution) Technologien, und zwar QKD mit Quantenverschränkung, QKD mit Polarisierung einzelner Photonen und QKD mit einem kontinuierlichen Photonen-Strom, sowie RKD (Radio-signal Key Distribution), das auf der Reziprozität einer normalen Funkübertragung basiert, und MKD (Memory Key Distribution), das hochsichere Speichermedien, Chipkarten und ein One-Time Pad verwendet. Die QKD-Technologien werden mit Lichtleitern und Satelliten behandelt.

Nach einer verständlichen Beschreibung werden diese Technologien nach Leistungskriterien der Praxis verglichen und der Praxiseinsatz für die Telekommunikation und Datenspeicherung behandelt.

Dadurch werden erstmals in einer Studie und einem Fachbuch diese fünf Technologien dargestellt und technologieneutral verglichen und es wird gezeigt, dass zu QKD mit RKD und MKD sehr interessante Alternativen mit vergleichbarer Sicherheit existieren.

Neben der mathematischen Kryptografie, die auf mathematischen Verfahren basiert, gibt es auch eine physikalische Kryptografie auf Basis der Physik. Die Sicherheitsbeurteilung mathematischer Verfahren der Kryptografie basiert auf Vermutungen und ist daher abhängig von der aktuellen Kenntnis von Angriffsmethoden und der Rechenleistung der Angreifer. Mit den physikalischen Verfahren wird ein neues Paradigma der Kryptographie eingeführt, das sich von der heutigen komplexitätsbasierten Kryptographie abhebt. Die Verfahren sind sicher gegen rechnerisch sehr starke Gegner, wie z.B. leistungsstarke Quantencomputer oder optische Computer, und heute noch der Fachwelt unbekannte mathematische Angriffsmethoden, d.h. sicher gegen noch unveröffentlichte mathematische Verfahren, die heutige mathematische Verfahren inklusive der Post-Quanten Kryptografie brechen können.

Digitalisierung, Globalisierung und weltweite Vernetzung erfordern eine sichere Telekommunikation und Datenspeicherung,

was wiederum eine sichere Kryptografie erfordert. Wer mathematische Verfahren der Kryptografie aufgrund der auf Vermutungen basierenden Sicherheit ablehnt, insbesondere wenn es sich um Unternehmensdaten (wie z.B. Forschungsdaten, strategische Daten und Angebote), medizinische Daten, vertrauliche / geheime / streng geheime Daten von Staaten, Militärs etc. handelt, muss physikalische Verfahren verwenden.

Die Studie stellt den Stand der Technik der physikalischen Verfahren der Kryptografie auf leicht verständliche Weise vor und vergleicht die fünf wichtigen Technologien technologieneutral unter den Gesichtspunkten Marktreife, IT-Sicherheit, Kommunikationsentfernungen, Schlüsselraten, Eignung für bewegliche Objekte, Kosten, Robustheit, Standardisierung, Authentifikation und Nachteile. Des Weiteren behandelt die Studie die Umsetzung der Sicherheitsziele Vertraulichkeit (mit Datenverschlüsselung), Integrität (mit Message Authentication Codes) und Authentizität der Daten durch physikalische Kryptografie und den dafür erforderlichen Einsatz von Mathematik. Darüber hinaus befasst sich die Studie ausführlich mit der praktischen Umsetzung der physikalischen Kryptografie bei der Telekommunikation und Datenspeicherung.

Projektkoordinator

- Hochschule für Angewandte Wissenschaften St. Pölten GmbH

Projektpartner

- Bundesministerium für Landesverteidigung
- Bundeskanzleramt