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**	abgeschlossen
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 wurde in erster Linie verfasst für Leser, die in ihrem Umfeld eine sehr hohe Datensicherheit benötigen bzw. die sich für sehr hohe Datensicherheit und/oder Kryptografie interessieren. Sie behandelt mehrere QKD (Quantum Key Distribution) Technologien, und zwar QKD mit Verschränkung, DV-QKD mit Polarisierung einzelner Photonen und CV-QKD mit einem kontinuierlichen Photonen-Strom, sowie RKD (Radio-signal Key Distribution), das auf der Reziprozität einer Funkübertragung basiert, und MKD (Memory Key Distribution), das Chipkarten und spezielle Speichermedien verwendet.

Nach der allgemein verständlichen Beschreibung dieser fünf Technologien erfolgt ein technologieneutraler und objektiver Leistungsvergleich unter den Gesichtspunkten Marktreife, IT-Sicherheit, Kommunikationsentfernungen, Schlüsselraten, Eignung für bewegliche Objekte, Kosten, Robustheit, Standardisierung, Authentifikation und Nachteile. Darüber hinaus befasst sich die Studie mit der praktischen Umsetzung der physikalischen Verfahren der Kryptografie bei der Telekommunikation und Datenspeicherung.

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..

Der Vergleich der betrachteten fünf Technologien zeigt, dass physikalische Verfahren zur Erzeugung und Verteilung kryptografischer Schlüssel kein einheitliches Lösungsfeld bilden, sondern unterschiedliche sicherheitstechnische und organisatorische Konzepte repräsentieren. DV-QKD, CV-QKD und verschränkungsbasierte QKD teilen das grundlegende Ziel,

die Erzeugung und Verteilung der Schlüssel über einen physikalischen Übertragungskanal abzusichern, unterscheiden sich jedoch in technischer Ausgestaltung, erreichbarer Leistung und operativer Komplexität. RKD und MKD verfolgen demgegenüber Ansätze, bei denen Sicherheit primär aus physikalischen Eigenschaften von Geräten, Funkkanälen oder Prozessen sowie aus organisatorischen Maßnahmen resultiert.

QKD zeichnet sich durch einen hohen Grad formaler Absicherung auf Protokollebene aus, der unter idealisierten Annahmen weitreichende sicherheitstheoretische Aussagen erlaubt. Diese Stärke geht jedoch mit strukturellen Einschränkungen einher. Die erzielbaren Schlüsselraten sind begrenzt und stark abhängig von Distanz, Dämpfung und Betriebsbedingungen. Zudem erfordern Aufbau und Betrieb komplexe Systeme mit empfindlichen Komponenten, kontinuierlicher Kalibrierung und enger Überwachung. Die praktische Einsetzbarkeit ist daher häufig auf klar definierte Szenarien beschränkt, in denen Infrastruktur, Umgebung und Betrieb kontrollierbar sind.

RKD nimmt eine Zwischenstellung ein. Der Ansatz nutzt physikalische Eigenschaften von Funkkanälen, um Schlüssel zu extrahieren, verzichtet jedoch auf die formalen Sicherheitsgarantien quantenbasierter Protokolle. Die Stärken von RKD liegen in den vergleichsweise sehr geringen Kosten und technischen Komplexität. Dem stehen sehr niedrige Schlüsselraten und Entfernungen und Dynamikanforderungen (Bewegung zumindest eines Gerätes) gegenüber, was den Einsatz auf Nischenanwendungen beschränkt.

MKD unterscheidet sich strukturell am deutlichsten von den anderen Ansätzen. Hier wird die Erzeugung und Verteilung der Schlüssel zeitlich und räumlich vom eigentlichen Einsatz entkoppelt. Sehr große Mengen von Schlüsselmaterial können unabhängig von Übertragungskanälen erzeugt und anschließend physisch verteilt werden. Daraus ergeben sich sehr hohe effektiv verfügbare Schlüsselmengen bei vergleichsweise sehr geringer technischer Komplexität im laufenden Betrieb und geringen Kosten. Gleichzeitig verlagert sich der sicherheitsrelevante Aufwand in den organisatorischen Bereich: sichere Erzeugung, Lagerung, Transport und Verwaltung der Datenträger werden zu den zentralen Stellgrößen, die aber ohne speziellen Know-how einfach überwachbar und kontrollierbar sind.

Die charakteristischen Stärken und Schwächen der Ansätze lassen sich daher nicht isoliert, sondern nur im Zusammenspiel betrachten. Quantenbasierte Verfahren bieten konzeptionell elegante Lösungen für den kontinuierlichen Schlüsselaustausch über Distanz, sind jedoch sehr kostenintensiv und betrieblich anspruchsvoll. RKD stellt eine technisch einfache, aber leistungsmäßig stark eingeschränkte Alternative dar, kann aber bei bewegten Geräten und den Kosten punkten. MKD bietet außergewöhnlich hohe Schlüsselkapazitäten, die zur Verschlüsselung auch ein One-Time-Pad und damit eine 100%ig sichere Datenverschlüsselung ermöglichen, und robuste Betriebsbedingungen bei geringen Kosten. Die Herausforderungen liegen in der Skalierung, Organisation und logistischen Umsetzung.

Für eine übergreifende Einordnung ist schließlich entscheidend, dass sich die Technologien nicht nur in Leistungsparametern unterscheiden, sondern in ihrem grundlegenden Systemverständnis. Während QKD-Ansätze und RKD die Sicherheit primär als Eigenschaft eines laufenden physikalischen Übertragungsprozesses begreifen, verlagert MKD sicherheitsrelevante Fragestellungen bewusst in einen Bereich, der durch Prozesse, Verantwortlichkeiten und Kontrolle geprägt ist.

Projektkoordinator

- Hochschule für Angewandte Wissenschaften St. Pölten GmbH

Projektpartner

- Bundesministerium für Landesverteidigung
- Bundeskanzleramt