NSPT-QKD

Numerical security proof toolkit for quantum key distribution

Programm / Ausschreibung	Digitale Technologien, Digitale Technologien, Digitale Schlüsseltechnologien: Ausschreibung 2023	**Status**	laufend
Projektstart	01.12.2024	**Projektende**	30.11.2027
Zeitraum	2024 - 2027	**Projektlaufzeit**	36 Monate
Keywords	Quantum Key Distribution; Building Trust through Regulation (Cyber Resilience Act, NIS-2); Quantum Governance; Quantum Technologies; Numerical Security-Proof Toolkit		

Projektbeschreibung

Die Digitalisierung nimmt immer schneller Fahrt auf und die Anzahl vernetzter Geräte nimmt immer weiter zu. Dieses Wachstum erfordert robuste Sicherheitslösungen, insbesondere zum Schutz sensibler Daten, die im Internet übertragen werden. Die derzeit etablierten (klassischen) Verschlüsselungstechniken bergen jedoch potenzielle Sicherheitslücken aufgrund zukünftiger Fortschritte im Bereich von Quantencomputern und sich ständig weiterentwickelnder Hacking-Methoden.

Quantum Key Distribution (QKD) stellt sich als vielversprechende Alternative heraus. Sie nutzt die einzigartigen Eigenschaften der Quantenmechanik, um eine informationstheoretisch sichere Verschlüsselung zu erreichen. Obwohl das Feld seit seiner Entstehung bedeutende Fortschritte gemacht hat, besteht eine entscheidende Lücke zwischen den idealen, mathematisch sicheren QKD-Protokollen und ihrer praktischen Umsetzung mit realer Hardware.

In Anerkennung dieser Herausforderung betonen europäische Vorschriften die Bedeutung der Förderung einer sicheren Entwicklung von Quantentechnologien. Der Aufbau von Vertrauen in diese neue Technologie erfordert die Schließung dieser Lücke zwischen Theorie und Praxis und die Gewährleistung der gleichen Sicherheitsstandards wie bei traditionellen Verschlüsselungsmethoden.

Dieses Projekt schlägt einen interdisziplinären Ansatz vor, um diese Lücke zu schließen. Unsere Ziele sind:

– Entwicklung eines Open-Source-Software-Toolkits, das numerische Sicherheitsnachweise verwendet, um QKD-Systeme unter realistischen Bedingungen und unter Berücksichtigung von Hardwarebeschränkungen zu analysieren.
– Nutzung bestehender Cybersicherheits-Frameworks, um Erkenntnisse in praktische Empfehlungen für sichere QKD-Implementierungen umzusetzen.
– Förderung des Vertrauens in QKD durch die Schließung der Lücke zwischen theoretischer Sicherheit und praktischer

Implementierung.

Dieses Projekt bietet verschiedene innovative Aspekte:

– Numerische Sicherheitsnachweise: Analyse von QKD-Systemen mit praktischen Imperfektionen, um den Weg für klare Sicherheitsstandards zu ebnen.
– Open-Source-Software-Toolkit: Behebung von Einschränkungen bestehender Tools und Ermöglichung effizienter Sicherheitsanalysen verschiedener QKD-Protokolle.
– Praktische Empfehlungen: Bereitstellung von Best Practices und regulatorischen Leitlinien für sichere QKD-Implementierungen in der realen Welt.

Die erwarteten Ergebnisse umfassen:

– Ein Software-Toolkit, das eine zuverlässige Sicherheitsanalyse verschiedener QKD-Protokolle ermöglicht.
– Best Practices und regulatorische Empfehlungen für sichere Implementierungen spezifischer QKD-Protokolle.
– Gesteigertes Vertrauen in die QKD-Technologie durch die Zusammenarbeit von Industrie und Wissenschaft sowie praktische Sicherheitsbewertungen.

Dieses Projekt fördert Innovationen durch Zusammenarbeit und adressiert direkt den Bedarf an vertrauenswürdigen QKD-Lösungen. Durch die erfolgreiche Überbrückung der Kluft zwischen Theorie und Praxis ebnet dieses Projekt den Weg für QKD, ein Eckpfeiler der Cybersicherheitslösungen der nächsten Generation zu werden und die technologische Souveränität und Wettbewerbsfähigkeit Europas im Quantenzeitalter zu stärken.

Abstract

Our digital world is rapidly expanding, with connected devices experiencing a surge. This growth necessitates robust security solutions, particularly for protecting sensitive data traversing the internet. Traditional cryptography, while well-established, faces potential vulnerabilities from future advancements in quantum computing and ever-evolving hacking techniques.

Quantum Key Distribution (QKD) emerges as a promising answer, harnessing the unique properties of quantum mechanics to achieve information-theoretically secure communication. While the field has witnessed significant progress since its inception, a critical gap exists between the ideal, mathematically secure QKD protocols and their practical implementation with real-world hardware imperfections.

Recognizing this challenge, European regulations emphasize the importance of fostering secure QKD development. Building trust in this new technology requires addressing this gap and ensuring the same level of scrutiny applied to traditional encryption methods.

This project proposes an interdisciplinary approach to bridge this gap. We aim to:

– Develop an open-source software toolkit utilizing numerical security proofs to analyze QKD systems under realistic

conditions, incorporating hardware limitations.
– Leverage existing cybersecurity frameworks to translate insights into practical recommendations for secure QKD deployments.
– Foster trust in QKD by bridging the gap between theoretical security and practical implementation.

This project offers several innovative aspects:

– Numerical security proofs: Analyzing QKD systems with practical imperfections, paving the way for clear security standards.
– Open-source software toolkit: Addressing limitations of existing tools and enabling efficient security analysis of diverse QKD protocols.
– Practical recommendations: Providing best practices and regulatory guidance for secure real-world QKD implementations.

The expected outcomes include:

– A software toolkit facilitating reliable security analysis of various QKD protocols.
– Best practices and regulatory recommendations for secure deployments of specific QKD protocols.
– Increased trust in QKD technology through industry-academia collaboration and practical security assessments.

This project fosters innovation through collaboration and directly addresses the need for trustworthy QKD solutions. By successfully bridging the gap between theory and practice, this project paves the way for QKD to become a cornerstone of next-generation cybersecurity solutions, strengthening European technological sovereignty and economic competitiveness in the quantum era.

Projektkoordinator

- Quantum Technology Laboratories GmbH

Projektpartner

- Technische Universität Wien
- Universität Innsbruck