TU Berlin – Security in Telecommunications

FLOQI Abschlussbericht

ZE: TU Berlin	Förderkennzeichen: 16KIS1072
Vorhaben: Full Lifecycle Post-Quantum PKI - FLOQI	
Bewilligungszeitraum: 01.12.2019 – 30.11.2022	
Berichtszeitraum: 01.12.2019 – 31.12.2022	

1 Kurze Darstellung des Vorhabens

Kryptografische Verfahren werden eingesetzt, um Schutzziele wie Vertraulichkeit und Integrität in Anwendungen zu erreichen. Es ist bekannt, dass kryptografische Verfahren nicht immer sicher bleiben: sie „altern“ mit der Zeit. Das liegt zum einen an besseren Angriffe auf deren Strukturen und zum anderen bedrohen Quantencomputer heutige kryptografische Verfahren. Kryptografische Agilität (kurz: Krypto-Agilität) ermöglicht einen einfachen Wechsel der kryptografischen Funktionalität. Dies ist besonders wichtig in Produkten mit einer langen Lebensdauer, bspw. liegt die durchschnittliche Produktlebenszeit im Bereich der Produktion bzw. Automatisierung bei 10 bis 20 Jahren. Das Projekt „Full Lifecycle Post-Quantum PKI” hat es sich dementsprechend zum Ziel gesetzt, eine abwärtskompatible, quantencomputerresistente PKI zu entwerfen.

Motivation und Hintergrund

Über Public-Key-Infrastrukturen (PKI) können Entitäten sicher öffentlichen Schlüsseln zugeordnet und somit verifiziert werden. PKIs nutzen hierfür assymettische Kryptographie auf der Basis des Problems der Faktorisierung des Diskreten Logarithmus. Die Entwicklung bei Quantencomputern hat aber bereits jetzt eine erhebliche Auswirkung auf die Sicherheit aktuell eingesetzter asymmetrischer Krypto-Verfahren. Shors Algorithmus kann eingesetzt werden, um aktuell eingesetzte asymmetrische Verfahren zu brechen. Es müssen dementsprechend Alternativen entwickelt werden, um auf die Entwicklung von Quantencomputern vorbereitet zu sein.

Kryptografische Agilität (kurz: Krypto-Agilität) ermöglicht einen einfachen Wechsel der kryptografischen Funktionalität. Dies ist besonders wichtig in Produkten mit einer langen Lebensdauer, bspw. liegt die durchschnittliche Produktlebenszeit im Bereich der Produktion bzw. Automatisierung bei 10 bis 20 Jahren. Durch Initiativen wie Industrie 4.0 (I4.0) kann man eine starke Zunahme der vernetzten Komponenten innerhalb von Produktionsanlagen beobachten. Dadurch sind Industrieanlagen nicht wie bisher von der Außenwelt abgeschottet, sondern mit dem Internet (z.B. Cloud-Diensten) und Office-Umgebungen verbunden. Dieser Trend der Vernetzung ist auch im Bereich der Automobilindustrie zu beobachten und wird auch in Zukunft anhalten, wodurch deutlich mehr schützenswerte Daten, wie Prozessdaten, Steuerungsdaten, Sensorwerte, Fehlinformationen und Arbeitspläne, die Produktionswelt verlassen und bspw. in Cloud-Diensten gespeichert werden. Damit die Kommunikation zwischen I4.0-Produkten und Cloud-Diensten angesichts der Bedrohung durch Quantencomputer über die gesamte Lebensdauer abgesichert werden kann, ist es notwendig bereits in der Entwicklungsphase Krypto-Agilitätsstrategien anzuwenden. Ein wichtiger Bestandteil ist das Vorhandensein einer sicheren Methode zum Update der kryptografischen Funktionalität durch bspw. Over-The-Air (OTA) Firmware Updates. Das Finanzwesen ist eine der kritischen Infrastrukturen, auf die sich in besonderem Maße in fast allen Lebensbereichen verlassen wird.

Es besteht also in verschiedensten Industrien natürlicherweise ein besonders hoher Schutzbedarf, der langfristig effektive Mechanismen erfordert. PQ-Verfahren stellen hier das Mittel der Wahl dar, um den Schutz dieser kritischen Infrastruktur auch im Zeitalter der Quantencomputer gewährleisten zu können.

Ziele des Projekts

Das Hauptziel des Projekts FLOQI war es, eine abwärtskompatible, quantencomputerresistente PKI zu entwerfen.

1. **Anforderungsanalyse PQ-PKI**: Zuerst sollte ermittelt werden, welche Anforderungen eine Post-Quantum PKI erfüllen muss. Dazu zählen die Voraussetzungen, insbesondere hinsichtlich Abwärtskompatibilität, die ein hybrides Zertifikat erfüllen muss und auch Anforderungen an einen Parallelbetrieb einer klassischen und Post-Quantum-PKI. Außerdem werden die zur Verfügung stehenden Ressourcen auf heutigen Sicherheitschips und eingebetteten Systemen erhoben, um eine Grundlage zur Auswahl geeigneter kryptographischer Verfahren zu schaffen.
2. **Auswahl von Post-quantum Signaturkandidaten**: Als nächstes sollten sollen aktuelle quantencomputerresistente Signaturverfahren hinsichtlich Sicherheit und Performanz untersucht werden. Auf Grundlage der für die PQ-PKI definierten Anforderungen werden dann geeignete Verfahren ausgewählt, auch im Hinblick darauf, dass für jedes Verfahren passende Parameter gewählt werden, welche die Anforderungen an die benötigten Sicherheitsniveaus, sowie Ressourcenbeschränkungen erfüllen.
3. **Spezifikation und Implementierung der PQ-PKI**: Auf der Basis der vorrausgegangen Analysen sollte nun eine kryptoagile und hybridge PQ-PKI spezifiezierst und implementiert werden. Diese soll so konstruiert werden, dass sie flexibel in verschiedenen Bereichen einsetzbar ist. Außerdem wird der Parallelbetrieb von klassischen und Post-Quantum PKIs spezifiziert.
4. **Bedrohungsanalyse existierenden Verfahren:** Anschließend sollte eine soll eine Bedrohungsanalyse für die verschiedenen Verfahren durchgeführt werden. Hierbei lag der Fokus insbesondere auf Seitenkanalverfahren.

Projektverlauf und Methodik

Der Verlauf des Projekts wurde durch eine systematische und iterative Vorgehensweise geprägt. Zu Beginn wurden umfassende Literaturrecherchen und Analysen durchgeführt, um den aktuellen Stand der Forschung im Bereich der quantencomputerresistenten Kryptographie zu ermitteln. Diese Erkenntnisse bildeten die Grundlage für die Entwicklung der PQ-PKI und die Priorisierung der

Kryptographieverfahren, die in der PQ-PKI implementiert und evaluiert werden sollten.

Im nächsten Schritt wurden die angepeilte PQ-PKI spezifiziert und implementiert. Es ging eine effiziente, beweisbar sichere Implementierung hervor, deren Designabwägungen in mehreren Dokumenten erklärt worden ist. Die Ergebnisse wurden in wissenschaftlichen Publikationen dargestellt. Die Signaturverfahren, die für die PQ-PKI umgesetzt wurden, wurden anhand des vorangegangen Schrittes ausgewählt.

Es wurden zusätzlich Bedrohungs-und Risikoanalysen der ausgewählten und potentieller Verfahren durchgeführt.

Bedeutung und Ausblick -- Darstellung des voraussichtlichen Nutzens

Die Ergebnisse des Projekts FLOQI tragen wesentlich zur Vorbereitung auf eine post-quantitative Zukunft bei. Durch die Entwicklung und Integration einer post-quantum Public-Key-Infrastruktur (PKI) wird Entwicklern eine leistungsfähige und flexible Plattform zur Verfügung gestellt, um sichere Kommunikations- und Datensicherheitslösungen zu entwickeln. Die erreichte Kryptoagilität stellt sicher, dass die Infrastruktur auch zukünftig anpassungsfähig bleibt und neue Bedrohungen schnell und effizient adressiert werden können.

Die im Projekt erzielten Fortschritte und Erkenntnisse sind nicht nur für die Wissenschaft und Forschung von Bedeutung, sondern haben auch direkte Auswirkungen auf die Praxis. Unternehmen und Organisationen, die auf die post-quantum PKI setzen, profitieren unmittelbar von den erweiterten Sicherheitsfunktionen und können auf der entwickelten Implementierung aufbauen. Die entwickelten Angriffe helfen dabei, die Bedrohungslandschaft für PQ-Verfahren zu verstehen und Implementierung besser gegen diese schützen zu können.

Somit wurde durch das Projekt eine Basis für weiterführende Forschung und Entwicklung im Bereich der quantencomputerresistenten Kryptographie geschaffen. Zukünftige Arbeiten können auf den Ergebnissen dieses Projekts aufbauen und weiterführende Optimierungen und Erweiterungen vornehmen.

Das Projekt FLOQI ist somit ein wichtiger Schritt auf dem Weg zu einer sicheren digitalen Zukunft. Die erfolgreiche Implementierung quantencomputerresistenter Algorithmen und die Verbesserung der Kryptoagilität und Benutzbarkeit der Infrastruktur sind entscheidende Meilensteine, um den Herausforderungen einer zukünftigen Quantencomputer-Ära gerecht zu werden.

Zusammenarbeit mit anderen Stellen

Das Projekt fand statt unter der Leitung des Fraunhofer AISEC, in Zusammenarbeit mit der operational services GmbH & Co. KG, der Bundesdruckerei, ESCRYPT, der Robert Bosch GmbH, dem Unternehmen Dieblold Nixdorf sowie der BMW Group. Zudem gab es einen regen Austausch mit dem Projekt KBLS, sowie einen Austauschen ihm Rahmen der physischen und virtuellen PQC-Vernetzungstreffen.

2 Eigehende Darstellung der Vorhabensergebnisse

2. 1 Verwendung der Zuwendung

Die Zuwendungen wurden entsprechend dem Arbeits- und Finanzierungsplan des Projektantrages eingesetzt.

2.2 Ergebnisse des Vorhabens

Evaluierung von post-quantum Kryptographieverfahren

Um zu evaluieren, welche Verfahren für die hybride PKI geeignet sind, orientierte sich das Projekt an dem – zum Start des Projekt noch nicht abgeschlossenem - Standardisierungsprozess der National Institute of Standards and Technology (NIST) erschwert, der zu Beginn des Projekts in vollem Gange war und sich weiterhin verzögerte. Der Standardisierungsprozess ist von entscheidender Bedeutung für die Auswahl und Implementierung sicherer und zukunftsfähiger kryptographischer Verfahren. Daher bestand der erste große Meilenstein des Projekts in einer umfassenden Literaturrecherche und einem systematischen Zusammentragen aller verbliebenen Post-Quantum-Kandidaten der NIST.

Diese Recherche umfasste die Identifizierung und Dokumentation relevanter Parameter aller in Betracht kommenden Verfahren. Die Ergebnisse wurden in einer frei zugänglichen Datenbank zusammengefasst, die Entwicklern nicht nur im Rahmen von FLOQI, sondern auch darüber hinaus, eine wertvolle Orientierungshilfe bietet. Diese Datenbank wurde im Verlauf des Projekts mehrfach aktualisiert, um den neuesten Stand der Forschung zu reflektieren.

Spezifikation und Implementierung einer PQ-PKI Im Rahmen des Projektes FLOQI wurde eine gemischte PQ-PKI spezifiziert, inklusive Sicherheitsbeweis. Entsprechend der Ergebnissen aus der Analyse der PQ-Verfahren wurde diese PQ-PKI auf Basis der Verfahren XMSS und Dilithium umgesetzt. Die PQ-PKI wurde mit Hilfe der Bibliothek WolfSSL implementiert und evaluiert. Die Leistung dieser Lösung wurde evaluiert, mit dem Ergebniss dass dass sie die Zeit der Signaturüberprüfung erheblich reduziert und die Größe der Vertrauenskette minimiert.

Bedrohungsanalyse der PQ-Signaturverfahren Die Bedrohungsanalyse der existierenden PQ-Signaturverfahren wurde erfolgreich durchgeführt und entwickelte bis dahin unbekannte Angriffsszenarien für mehrere Verfahren. Diese Angriffe liefern wertvolle Erkenntnisse darüber, welchen Ansprüchen Implementierungen genügen müssen, um gegenüber Seitenkanalangriffen resistent zu sein. Im Rahmen dieser Untersuchungen wurden neuartige Angriffsmethoden entwickelt, insbesondere wie durch den Einsatz von Machine Learning und neuartigen Schlüsselrekonstruktionsverfahren komplexe Angriffe möglich sind, die selbst geschützte Implementierungen brechen können. Diese neuen Angriffe geben eine klare Übersicht über die Bedrohungslage und die erforderlichen Gegenmaßnahmen.

2.3 Ausführliche Darstellung der Vorhabensergebnisse

Literaturrecherche und Datenbank der Post-Quantum-Kandidaten

Der erste große Meilenstein des Projekts bestand in der ausführlichen Literaturrecherche und dem systematischen Zusammentragen aller verbliebenen Post-Quantum-Kandidaten der NIST. Diese Arbeit war von entscheidender Bedeutung, um eine fundierte Grundlage für die weitere Entwicklung zu schaffen. Die relevanten Parameter der verschiedenen Verfahren wurden identifiziert und in einer umfassenden Datenbank dokumentiert.

Diese Datenbank bietet Entwicklern eine ausgezeichnete Orientierungshilfe, um das für ihren jeweiligen Anwendungszweck am besten geeignete Verfahren auszuwählen. Sie enthält detaillierte Informationen zu den Sicherheitsparametern, der Performance und den Implementierungsanforderungen der verschiedenen Post-Quantum-Algorithmen. Darüber hinaus wurde die Datenbank im Verlauf des Projekts mehrfach aktualisiert, um den neuesten Stand der Forschung und die aktuellen Entwicklungen im Standardisierungsprozess zu berücksichtigen.

Spezifikation und Implementierung der PQ-PKIen

Es wurde eine Spezifikation für die Struktur von gemischten X.509-Zertifikaten geschaffen. Vorschläge aus der Literatur wurden evaluiert und diskutiert. Auf dieser Basis wurde ein Konzept für eine Post-Quantum-PKI entworfen, das flexibel in verschiedenen Bereichen einsetzbar ist. Zudem wurde der Parallelbetrieb von klassischen und Post-Quantum PKIs spezifiziert.

Die entwickelte Lösung ist eine gemischte PKI (statt einer hybriden PKI). Die Entscheidung begründen wir in einem guten Literaturüberblick. Wir erkären zusätzlich den Unterschied zwischen diesen beiden Konzepten.

Unsere Lösung wurde erfolgreich in WolfSSL implementiert und der Code auf Github veröffentlicht.

Bedrohungsanalyse

Bei der Risikoanalyse konzentrierte sich das Projekt auf die Anfälligkeit der Post-Quantum-Verfahren für Seitenkanalangriffe. Das Projekt hat dabei vier Verfahren insbesondere evaluiert: Rainbow und MAYO, ein multivariates Signaturverfahren sowie BLISS und Dilithium, beides Gitterbasierte Verfahren. Für Rainbow konnte das Projekt Anfälligkeit für Fehlerinjektionsangriffe zeigen, für MAYO haben wir ihm Rahmen des Projekts eine Fehlerinjektions-resistente Hardware implementierung entwickelt. Sowohl für BLISS als auch Dilithium konnten wir Seitenkanalangriffe demonstrieren, die zur Schüsselwiederbeschaffung führen. Wir haben in diesem Rahmen auch haben auch drei verwandte Energie-Seitenkanal-Angriffe auf GALACTICS, eine Konstant Zeit-Implementierung von BLISS, vorgestellt. Alle Angriffe basieren auf Leakage, die wir im Gaussian Sampling- und Signieralgorithmus von GALACTICS identifiziert haben. Zur Durchführung des Angriffs ist eine Profiling-Phase auf einem Gerät erforderlich, das mit dem angegriffenen Gerät identisch ist, um Klassifikatoren für maschinelles Lernen zu trainieren. In der Angriffsphase ermöglichen die Leakages in GALACTICS den trainierten Klassifikatoren, sensible interne Informationen mit hoher Genauigkeit vorherzusagen, was den Weg für drei verschiedene Schlüsselwiederherstellungsangriffe ebnet. Wir demonstrieren die Leakages, indem wir GALACTICS auf einem Cortex-M4 laufen lassen und stellen Proof-of-Concept-Daten und eine Implementierung für alle unsere Angriffe bereit. Diese Angriffe geben Aufschluss darüber, welchen Ansprüchen Implementierungen genügen müssen, um gegenüber Seitenkanalangriffen resistent zu sein. Wir haben ihm Rahmen dieser Angriffe zum einen demonstriert, wie durch machine-learning und neuartige Schlüsselrekonstruktionsverfahren komplexe Angriffe durchgeführt werden können, die selbst geschütze Implementierungen brechnen können. Die Angriffe wurden im Rahmen mehrere Publikation veröffentlicht, die Implementierung der Angriffe sowie der Gegenmaßnahmen wurden ebenfalls veröffentlicht.

2.4 Wichtigste Positionen des Zahlenmäßigen Nachweises

Die Gesamtförderung betrug 399.882,00€. Darin enthalten sind Personalkosten in Höhe von 322.937,00€, Reisekosten von 10.000,00€, Gegenstandskosten von 298,00€ sowie eine Projektpauschale von 66.647,00€.

2.5 Notwendigkeit und Angemessenheit der geleisteten Arbeit

Die erbrachten Forschungs- und Entwicklungsarbeiten entsprechen in Umfang und erzielten Ergebnissen in vollem Umfang der Vorhabenbeschreibung.

2.6 Fortschritte auf dem Gebiet des Vorhabens bei anderen Stellen

Während der Durchführung des Projektes wurde insbesondere das Auswahlverfahren der NIST abgeschlossen und es wurden mehrere Angriffe gegenüber existierenden Verfahren veröffentlicht. Keine dieser Angriffe unterminieren die Sicherheit des Implementierten PQ-PKI, da XMSS und Dilithium weiterhin als sicher gelten. Die Bedrohungsanalyse hat sich den neuen Erkentnissen angepasst und auf die als sicher geltenden Verfahren konzentriert (z.B. auf MAYO statt auf Rainbow). Besonders hervorzuheben sind folgende Ergebnisse:

Rainbow und SIKE

Rainbow, ein multivariates quadratisches Signaturschema, galt lange Zeit als vielversprechend für Post-Quantum-Kryptographie. Es basiert auf der Schwierigkeit, multivariate quadratische Gleichungen über endlichen Körpern zu lösen. Trotz der theoretischen Robustheit gegenüber klassischen Angriffen und auch vielen bekannten Quantenangriffen, wurden Schwächen in seiner Konstruktion entdeckt. Forscher fanden Wege, die mathematischen Strukturen von Rainbow zu durchbrechen, was die Sicherheit dieses Verfahrens erheblich untergräbt.

SIKE, das auf isogeniebasierten Schlüsselvereinbarungsprotokollen basiert, war ein weiteres prominentes Verfahren, das in der Post-Quantum-Kryptographie-Bewegung eine wichtige Rolle spielen sollte. Es wurde angenommen, dass die Verwendung supersingulärer elliptischer Kurven und isogeniebasierter Schlüsselvereinbarung eine starke Sicherheit gegen Quantenangriffe bieten würde. Doch auch SIKE ist gebrochen worden. Dies bedeutet, dass die theoretische Basis, auf der SIKE aufgebaut wurde, nicht stark genug ist, um die versprochene Sicherheit zu gewährleisten. Diese Brüche haben erhebliche Auswirkungen auf die Post-Quantum-Kryptographie und erfordern eine Neubewertung der verwendeten Algorithmen und Methoden.

Alternative Signaturverfahren der NIST-Forum

Die NIST hat nach Abschluss ihres Auswahlverfahren einen weiteren Call For Proposals ausgerufen, da nur gittterbasierte Signaturverfahren ausgewählt wurden. FLOQI hat eines dieser alternativen Verfahren (MAYO) ebenfalls einer Untersuchung unterzoegen und auf Effizienz in der Hardware Implementierung untersucht. Zukünftige Forschung muss allerdings auch andere Verfahren in Betracht ziehen.

2.7 Erfolgte und geplante Veröffentlichungen der Ergebnisse

Ulitzsch, Vincent Quentin, et al. "A post-quantum secure subscription concealed identifier for 6G." *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 2022.

Marzougui, Soundes, et al. "Machine-learning side-channel attacks on the galactics constant-time implementation of bliss." *Proceedings of the 17th International Conference on Availability, Reliability and Security*. 2022.

Aulbach, Thomas, et al. "Recovering rainbow’s secret key with a first-order fault attack." *International Conference on Cryptology in Africa*. Cham: Springer Nature Switzerland, 2022.

Marzougui, Soundes, et al. "On the feasibility of single-trace attacks on the Gaussian sampler using a CDT." *International Workshop on Constructive Side-Channel Analysis and Secure Design*. Cham: Springer Nature Switzerland, 2023.

Sayari, Oussama, et al. "HaMAYO: A Fault-Tolerant Reconfigurable Ha rdware Implementation of the MAYO Signature Scheme." *International Workshop on Constructive Side-Channel Analysis and Secure Design*. Cham: Springer Nature Switzerland, 2024.

Ulitzsch, Vincent Quentin, et al. "Loop Aborts Strike Back: Defeating Fault Countermeasures in Lattice Signatures with ILP." *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2023.4 (2023): 367-392.

Marzougui, Soundes, and Jean-Pierre Seifert. "XMSS-based chain of trust." *Proceedings of 10th International Workshop on Security Proofs for Embedded Systems, EPiC Series in Computing*. Vol. 87. 2022.

Breaks, A. Small Bit-Fiddling Leak. "Profiling Side-Channel Attacks on Dilithium." *Selected Areas in Cryptography: 29th International Conference, SAC 2022, Windsor, ON, Canada, August 24–26, 2022, Revised Selected Papers*. Springer Nature.

TU Berlin, Sekr. TEL 16 | Ernst-Reuter-Platz 7 | 10587 Berlin

Adressat

Fakultät IV Elektrotechnik und Informatik
Institut für Softwaretechnik und Theoretische Informatik

Security in Telecommunications

Prof. Dr. phil. nat. Jean-Pierre Seifert

Sekretariat TEL 16
Ernst-Reuter-Platz 7
10587 Berlin

jpseifert@sect.tu-berlin.de

Administrative Assistenz
Andrea Hahn

secretary@sect.tu-berlin.de

Unser Zeichen:
TEL 16

Berlin, 03.07.2024

Kurzbericht Full Lifecycle Post-Quantum PKI (FLOQI)

Über Public-Key-Infrastrukturen (PKI) können Entitäten sicher öffentlichen Schlüsseln zugeordnet und somit verifiziert werden. PKIs nutzen hierfür assymettische Kryptographie auf der Basis des Problems der Faktorisierung des Diskreten Logarithmus. Die Entwicklung bei Quantencomputern hat aber bereits jetzt eine erhebliche Auswirkung auf die Sicherheit aktuell eingesetzter asymmetrischer Krypto-Verfahren. Durch einen Algorithmus von Shor von 1994 können das Problem der Faktorisierung und des Diskreten Logarithmus gelöst werden. Damit wären auf RSA, dem Diffie-Hellman-Schlüsseltausch oder DSA basierende Verfahren unsicher. Insbesondere besteht die Gefahr, dass vertrauliche Kommunikation bereits heute aufgezeichnet wird, um sie in Zukunft zu entschlüsseln, sobald Quantencomputer ausreichender Größe existieren. Weiterhin ist sichere Kommunikation auch für langlebige Geräte notwendig, bei denen sich eine nachträgliche Aktualisierung schwierig gestaltet. Dadurch entsteht die Notwendigkeit, jetzt schon den Umstieg auch Post-Quantum-Verfahren einzuleiten.

Ziel des Projekt FLOQI war es, eine abwärtskompatible PKI zu entwerfen, die Post-Quantum Verfahren nutzen kann. Insbesondere lag der Fokus auf der Evaluation der potentiellen post-quantum Kryptographieverfahren, die für eine solche PKI genutzt werden können. Außerdem wurden Lösungen basierend auf hybriden X.509 Zertifikaten betrachtet, die klassische und Post-Quantum Verfahren kombinieren, aber auch der Parallelbetrieb von konventionellen und Post-Quantum-PKIs untersucht und im Feld getestet.

Im Projekt wurden mehrere Arbeitspakete abgeschlossen, um dieses Ziel zu erreiche. Zuerst wurden PQC-Verfahren gesichtet und evaluiert. Um eine einfache und flexible Auswahl der PQ-Verfahren zu ermöglichen, wurden hierzu in Zusammenarbeit mit Fraunhofer AISEC und dem Projekt KBLS die Kandidaten der

TU Berlin, Sekr. TEL 16 | Ernst-Reuter-Platz 7 | 10587 Berlin

Fakultät IV Elektrotechnik und Informatik
Institut für Softwaretechnik und Theoretische Informatik

Security in Telecommunications

Prof. Dr. phil. nat. Jean-Pierre Seifert

Sekretariat TEL 16
Ernst-Reuter-Platz 7
10587 Berlin

jpseifert@sect.tu-berlin.de

Administrative Assistenz
Andrea Hahn

secretary@sect.tu-berlin.de

Unser Zeichen:
TEL 16

dritten Runde des NIST-Auswahlverfahrens gesichtet. Diese Kandidaten wurden in eine Datenbank übertragen, welche über ein Webinterface verfügbar ist und ermöglicht, auch für zukünftige Anforderungen schnell geeignete Verfahren ausfindig zu machen. In dem Dokument „State of the art and outlook on cryptanalysis of post-quantum signatures“ wurden die NIST-Kandidaten analysiert und diskutiert.

Eine gemischte PKI, welche XMSS- und Dilithium-Signaturverfahren. Im Rahmen des Projekts wurde ein Proof-of-Concept Implementierung basierend auf WolfSSL entwickelt. Darüber hinaus bewerten wir die Leistung unserer Lösung
und stellen fest, dass sie die Zeit der Signaturüberprüfung erheblich reduziert und die Größe der Vertrauenskette minimiert.

Zusätzlich wurden eine Risikoanalyse der Post-Quantum Verfahren durchgeführt. Zuerst wurde im Dokument „Welch’s Test Limitations", die Einschränkungen des Welch's Tests zur Erkennung undichter Instruktionen erklärt. Bei der Risikoanalyse konzentrierte sich das Projekt auf die Anfälligkeit der Post-Quantum-Verfahren für Seitenkanalangriffe. Das Projekt hat dabei vier Verfahren insbesondere evaluiert: Rainbow und MAYO, ein multivariates Signaturverfahren sowie BLISS und Dilithium, beides Gitterbasierte Verfahren. Für Rainbow konnte das Projekt Anfälligkeit für Fehlerinjektionsangriffe zeigen, für MAYO haben wir ihm Rahmen des Projekts eine Fehlerinjektions-resistente Hardware implementierung entwickelt. Sowohl für BLISS als auch Dilithium konnten wir Seitenkanalangriffe demonstrieren, die zur Schüsselwiederbeschaffung führen. Diese Angriffe geben Aufschluss darüber, welchen Ansprüchen Implementierungen genügen müssen, um gegenüber Seitenkanalangriffen resistent zu sein. Wir haben ihm Rahmen dieser Angriffe zum einen demonstriert, wie durch machine-learning und neuartige Schlüsselrekonstruktionsverfahren komplexe Angriffe durchgeführt werden können, die selbst geschütze Implementierungen brechnen können. Die Angriffe wurden im Rahmen mehrere Publikation veröffentlicht, die Implementierung der Angriffe sowie der Gegenmaßnahmen wurden ebenfalls veröffentlicht.

Insgesamt wurde im Rahmen des FLOQI Projekts also eine Evaluation aktueller Post-Quantum Kryptographie Kandidaten durchgeführt, eine gemischtes PKI Verfahren spezifiziert und implementiert, und eine Risikoanalyse der Kandidaten, mit besonderem Fokus auf die Resistenz gegenüber Seitenkanalangriffen durchgeführt.