TU Berlin – Security in Telecommunications

KBLS Abschlussbericht

ZE: TU Berlin	Förderkennzeichen: 16KIS1060
Vorhaben: Kryptobibliothek Botan für langlebige Sicherheit - KBLS	
Bewilligungszeitraum: 01.11.2019 – 31.10.2022, Verlängerung bis 31.10.2023	
Berichtszeitraum: 01.11.2019 – 31.10.2023	

1 Kurze Darstellung des Vorhabens

Die Sicherheit digitaler Informationen ist ein zentrales Anliegen in unserer zunehmend vernetzten Welt. Mit der rasanten Entwicklung der Informationstechnologie und dem bevorstehenden Aufkommen von Quantencomputern steht die Welt vor neuen Herausforderungen in Bezug auf die Kryptographie. Traditionelle kryptographische Verfahren, die derzeit die Grundlage für den Schutz unserer digitalen Kommunikation und Daten bilden, sind durch die Rechenleistung von Quantencomputern potenziell gefährdet. Angesichts dieser Bedrohung ist die Entwicklung und Implementierung quantencomputerresistenter Kryptographie von größter Bedeutung. In diesem Kontext wurde das Projekt "KBLS - Kryptobibliothek Botan für langlebige Sicherheit" ins Leben gerufen, um eine robuste und zukunftssichere Kryptobibliothek zu entwickeln, die den Anforderungen der Post-Quantum-Kryptographie (PQC) gerecht wird.

1..Motivation und Hintergrund

Die Kryptobibliothek Botan ist eine weit verbreitete, plattformübergreifende Open-Source-Kryptobibliothek, die Entwicklern eine breite Palette an kryptographischen Werkzeugen und Algorithmen zur Verfügung stellt. Botan zeichnet sich durch ihre Flexibilität und Modularität aus, was sie zu einer idealen Basis für die Integration neuer kryptographischer Verfahren macht. Mit dem Aufkommen von Quantencomputern, die in der Lage sein werden, bestimmte kryptographische Algorithmen effizient zu brechen, wie beispielsweise das RSA-Verschlüsselungssystem und das Diffie-Hellman-Schlüsselaustauschprotokoll, besteht ein dringender Bedarf an der Erforschung und Implementierung von Algorithmen, die gegen solche Angriffe resistent sind.

Quantencomputer nutzen die Prinzipien der Quantenmechanik, um Berechnungen durchzuführen, die für klassische Computer unerschwinglich wären. Dies eröffnet nicht nur Möglichkeiten für bedeutende Fortschritte in verschiedenen Wissenschafts- und Technologiebereichen, sondern stellt auch eine ernsthafte Bedrohung für die gegenwärtigen kryptographischen Systeme dar. Insbesondere Algorithmen wie Shor’s Algorithmus und Grover’s Algorithmus können klassische kryptographische Verfahren effizient brechen. Daher ist die Entwicklung und Implementierung von quantencomputerresistenten Algorithmen, die selbst den mächtigsten Quantencomputern standhalten können, von entscheidender Bedeutung für die zukünftige Datensicherheit.

1..Ziele des Projekts

Das Hauptziel des Projekts KBLS war es, die Botan-Kryptobibliothek um quantencomputerresistente kryptographische Algorithmen zu erweitern und sie dadurch für den Einsatz in einer zukünftigen Post-Quantum-Ära vorzubereiten. Diese Erweiterung umfasst mehrere spezifische Teilziele:

1. **Integration quantencomputerresistenter Algorithmen**: Dies umfasst die Implementierung von Signaturalgorithmen, Schlüsselaustauschprotokollen und Verschlüsselungsverfahren, die gegen Angriffe durch Quantencomputer resistent sind. Besonders im Fokus standen dabei hashbasierte, gitterbasierte, codebasierte und isogeniebasierte Verfahren.
2. **Kryptoagilität**: Die Fähigkeit der Bibliothek, flexibel zwischen verschiedenen kryptographischen Algorithmen zu wechseln, wurde als Schlüsselmerkmal identifiziert. Kryptoagilität ermöglicht es, Algorithmen bei Bedarf schnell zu ersetzen, ohne umfangreiche Änderungen an der Implementierung vornehmen zu müssen. Dies ist besonders wichtig in einer sich schnell entwickelnden Bedrohungslandschaft.
3. **Verbesserung des Schlüsselmanagements**: Sicheres Schlüsselmanagement ist eine zentrale Komponente jeder kryptographischen Lösung. Das Projekt zielte darauf ab, sichere Mechanismen zur Schlüsselerzeugung, -speicherung und -löschung zu entwickeln und zu integrieren, einschließlich der Nutzung von Hardware-Sicherheitsmodulen (HSMs) und hardwaregestützter Verschlüsselungstechniken.
4. **Benutzbarkeit und Sicherheit**: Eine hohe Usability ist entscheidend, um sicherzustellen, dass Entwickler kryptographische Funktionen korrekt und effizient nutzen können. Daher wurden im Rahmen des Projekts regelmäßig Usability-Tests durchgeführt, um die Benutzerfreundlichkeit der Botan-Bibliothek zu evaluieren und zu verbessern.

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 Auswahl und Priorisierung der Algorithmen, die in die Botan-Bibliothek integriert werden sollten.

Im nächsten Schritt wurden die ausgewählten Algorithmen implementiert und in die bestehende Infrastruktur der Bibliothek integriert. Dabei wurde besonderer Wert auf die Optimierung der Algorithmen gelegt, um deren Effizienz und Sicherheit zu maximieren. Parallel dazu wurden Mechanismen zur Unterstützung der Kryptoagilität entwickelt, um einen nahtlosen Wechsel zwischen verschiedenen Algorithmen zu ermöglichen.

Ein weiterer Schwerpunkt lag auf der Implementierung eines sicheren Schlüsselmanagements. Hierbei wurden Techniken zur sicheren Schlüsselerzeugung und -speicherung sowie zur Nutzung von Hardware-Sicherheitsmodulen erprobt und integriert. Diese Maßnahmen sollen sicherstellen, dass kryptographische Schlüssel stets geschützt und vor unbefugtem Zugriff sicher sind.

Regelmäßige Usability-Tests wurden durchgeführt, um sicherzustellen, dass die entwickelten Funktionen leicht zugänglich und nutzerfreundlich sind. Feedback aus diesen Tests wurde kontinuierlich in die Weiterentwicklung der Bibliothek eingebracht, um die Benutzerfreundlichkeit weiter zu steigern und mögliche sicherheitstechnische Fehler bei der Implementierung zu minimieren.

1..Bedeutung und Ausblick

Die Ergebnisse des Projekts KBLS tragen wesentlich zur Vorbereitung auf eine post-quantitative Zukunft bei. Durch die Integration quantencomputerresistenter Algorithmen in die Botan-Kryptobibliothek wird Entwicklern eine leistungsfähige und flexible Plattform zur Verfügung gestellt, um sichere Kommunikations- und Datensicherheitslösungen zu entwickeln. Die erreichte Kryptoagilität stellt sicher, dass die Bibliothek 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 Botan-Kryptobibliothek setzen, profitieren unmittelbar von den erweiterten Sicherheitsfunktionen und der verbesserten Benutzbarkeit.

Zudem 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 "KBLS - Kryptobibliothek Botan für langlebige Sicherheit" 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 Botan-Bibliothek sind entscheidende Meilensteine, um den Herausforderungen einer zukünftigen Quantencomputer-Ära gerecht zu werden.

1..Zusammenarbeit mit anderen Stellen

Das Projekt fand statt unter der Leitung des Fraunhofer AISEC, in Zusammenarbeit mit der Rohde & Schwarz Cybersecurity GmbH und Nexenio. Zudem gab es einen regen Austausch mit dem Projekt FloQI, sowie einen Austauschen ihm Rahmen der physischen und virtuellen PQC-Vernetzungstreffen.

2 Eigehende Darstellung der Vorhabensergebnisse

1..Verwendung der Zuwendung

Für das Projekt wurde aufgrund der Einschränkungen durch die Corona-Pandemie eine kostenneutrale Verlängerung um eine Jahr auf vier beantragt. Die Stelle blieb jedoch im vierten Jahr unbesetzt.

1.2.1 Ergebnisse des Vorhabens

1..Herausforderungen und Standardisierungsprozess

Das Projekt wurde durch den noch nicht abgeschlossenen 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 KBLS, 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.

1..Entwicklerinterviews und Pandemiebedingte Verzögerungen

Ein weiteres wichtiges Arbeitspaket bestand in der Durchführung ausführlicher Entwicklerinterviews. Ziel dieser Interviews war es, die Bedürfnisse und Wünsche sowie mögliche Hemmnisse von Entwicklern bei der Nutzung von Krypto-Bibliotheken zu ermitteln. Diese Interviews sollten ursprünglich im Frühjahr und Sommer 2020 stattfinden. Aufgrund der Einschränkungen durch die Corona-Pandemie konnten sie jedoch nur verzögert durchgeführt werden, was zu weiteren Verzögerungen in vielen nachgelagerten Arbeitspaketen führte.

Die Ergebnisse der Entwicklerinterviews lieferten wertvolle Einblicke, die in die Weiterentwicklung der Botan-Bibliothek einflossen. Insbesondere wurden Usability-Aspekte und die Integration neuer kryptographischer Verfahren adressiert, um den Anforderungen und Erwartungen der Entwicklergemeinschaft gerecht zu werden.

1..Hybride Verschlüsselung und Zertifikatsstandards

Für die hybride Verschlüsselung wurden Konzepte sowohl für Verschlüsselung als auch für Signaturen entwickelt. Das Ziel war es, Verfahren zu erarbeiten, die die Sicherheit klassischer und Post-Quantum-Verfahren kombinieren. Dabei zeigte sich, dass der derzeitige Standard X.509 für Zertifikate durch seine optionalen Felder bereits hybride Signaturen erlaubt. Diese Erkenntnis war entscheidend, um eine nahtlose Integration hybrider Verschlüsselungstechniken in bestehende Systeme zu ermöglichen.

1..Implementierung und wissenschaftliche Begleitung

Das größte Arbeitspaket des Projekts bestand in der Implementierung der quantenresistenten Algorithmen Kyber und Dilithium in die Krypto-Bibliothek Botan. Diese Implementierung wurde wissenschaftlich von der TU Berlin begleitet, um sicherzustellen, dass die höchsten Sicherheitsstandards eingehalten werden.

Während des Projekts wurden Seitenkanalangriffe durch Power Analysis bekannt, die im Team intensiv diskutiert wurden. Das abschließende Fazit war, diese Angriffe als „out of scope“ zu betrachten, da sie über die ursprünglichen Projektziele hinausgingen. Dennoch wurden mögliche Timing- und Cache-basierte Seitenkanalangriffe berücksichtigt und nach aktuellem wissenschaftlichen Erkenntnisstand ausgeschlossen.

Inzwischen sind Kyber und Dilithium erfolgreich in Botan implementiert und stehen Entwicklern zur Verfügung. Diese Implementierungen bieten eine robuste Grundlage für sichere Post-Quantum-Kryptographie und tragen dazu bei, die Botan-Bibliothek zu einer zukunftsfähigen und vielseitigen Krypto-Lösung zu machen.

1.2.2 Ausführliche Darstellung der Vorhabensergebnisse

1..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.

1..Entwicklerinterviews und Usability-Optimierung

Ein weiteres zentrales Arbeitspaket bestand in der Durchführung von Entwicklerinterviews. Diese Interviews zielten darauf ab, die Bedürfnisse, Wünsche und möglichen Hemmnisse von Entwicklern bei der Nutzung von Krypto-Bibliotheken zu ermitteln. Durch die Pandemiebedingten Einschränkungen konnten diese Interviews nur verzögert durchgeführt werden, was jedoch nicht minder wertvolle Erkenntnisse lieferte.

Die Ergebnisse der Interviews flossen direkt in die Weiterentwicklung der Botan-Bibliothek ein. Insbesondere wurden Aspekte der Benutzerfreundlichkeit und der Integration neuer kryptographischer Verfahren adressiert. Die Erkenntnisse halfen dabei, die Bibliothek so zu gestalten, dass sie den Anforderungen und Erwartungen der Entwicklergemeinschaft entspricht. Dies umfasste die Verbesserung der Dokumentation, die Bereitstellung von Beispielanwendungen und die Optimierung der Schnittstellen.

1..Konzepte für hybride Verschlüsselung

Ein weiteres bedeutendes Ergebnis des Projekts waren die Konzepte für hybride Verschlüsselung und Signaturen. Ziel dieser Arbeit war es, Verfahren zu entwickeln, die die Sicherheit klassischer und Post-Quantum-Verfahren kombinieren. Dies ist besonders wichtig, um eine reibungslose Übergangsphase zu gewährleisten, in der beide Arten von Verfahren parallel genutzt werden können.

Das Fazit dieser Arbeit war, dass der derzeitige Standard X.509 für Zertifikate durch seine optionalen Felder bereits hybride Signaturen erlaubt. Dies bedeutet, dass bestehende Systeme ohne größere Anpassungen erweitert werden können, um sowohl klassische als auch Post-Quantum-Signaturen zu unterstützen. Diese Erkenntnis erleichtert die Integration hybrider Verschlüsselungstechniken und trägt dazu bei, die Sicherheit von Kommunikationssystemen langfristig zu gewährleisten.

1..Implementierung von Kyber und Dilithium

Das größte und anspruchsvollste Arbeitspaket des Projekts war die Implementierung der quantenresistenten Algorithmen Kyber und Dilithium in die Krypto-Bibliothek Botan. Diese Arbeit wurde wissenschaftlich von der TU Berlin begleitet, um sicherzustellen, dass die höchsten Sicherheitsstandards eingehalten werden.

Während der Implementierungsphase wurden mögliche Seitenkanalangriffe intensiv untersucht. Insbesondere wurden Timing- und Cache-basierte Seitenkanalangriffe berücksichtigt und nach aktuellem wissenschaftlichen Erkenntnisstand ausgeschlossen. Seitenkanalangriffe durch Power Analysis wurden als „out of scope“ betrachtet, da sie über die ursprünglichen Projektziele hinausgingen.

Die Implementierung von Kyber und Dilithium ist inzwischen abgeschlossen, und beide Algorithmen sind in der Botan-Bibliothek verfügbar. Diese Implementierungen bieten eine robuste Grundlage für sichere Post-Quantum-Kryptographie und tragen

dazu bei, die Botan-Bibliothek zu einer zukunftsfähigen und vielseitigen Krypto-Lösung zu machen. Entwicklern steht nun ein leistungsfähiges Werkzeug zur Verfügung, um sichere und zukunftssichere Anwendungen zu entwickeln.

1.2.3 Fortschritte auf dem Gebiet des Vorhabens bei anderen Stellen

1..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.

1...Seitenkanalangriffe auf Dilithium

Ein weiteres Post-Quantum-Verfahren, das viel Beachtung gefunden hat, ist Dilithium, ein lattice-basierter Signaturalgorithmus. Lattice-basierte Verfahren gelten als besonders vielversprechend in der Post-Quantum-Kryptographie aufgrund ihrer Robustheit gegenüber den bekannten Angriffen sowohl klassischer als auch Quantencomputer. Allerdings ist auch Dilithium nicht frei von Schwächen. Insbesondere wurde festgestellt, dass Dilithium anfällig für Seitenkanalangriffe ist, die mittels Power-Analysis durchgeführt werden.

Seitenkanalangriffe nutzen physikalische Informationen, die während der Ausführung kryptographischer Operationen abgegriffen werden können. Power-Analysis ist eine spezielle Form von Seitenkanalangriffen, bei der der Energieverbrauch des Geräts während der kryptographischen Berechnungen analysiert wird, um geheime Schlüssel oder andere sensible Informationen zu extrahieren. Diese Art von Angriff kann sehr effektiv sein, insbesondere wenn sie gegen Implementierungen gerichtet ist, die nicht speziell gegen solche Angriffe gesichert sind.

In der Analyse von Dilithium wurde festgestellt, dass es Schwachstellen gibt, die durch Power-Analysis ausgenutzt werden können. Dies bedeutet, dass ein Angreifer, der physikalischen Zugang zu dem Gerät hat, auf dem Dilithium implementiert ist, in der Lage sein könnte, sensible Informationen zu extrahieren, die zur Kompromittierung der Sicherheit des Systems führen könnten.

1...Out-of-Scope-Betrachtung von Power-Analysis-Angriffen

Obwohl die Power-Analysis-Angriffe auf Dilithium eine reale Bedrohung darstellen, wurde im Rahmen des Projekts entschieden, diese Art von Angriffen als "out-of-scope" zu betrachten. Dies bedeutet, dass die Bedrohung durch Power-Analysis in der spezifischen Anwendungsumgebung und unter den gegebenen Projektzielen nicht in den Vordergrund gerückt wurde. Stattdessen lag der Fokus auf anderen Sicherheitsaspekten und Implementierungsdetails, die für den vorgesehenen Einsatz relevanter und unmittelbarer waren.

Die Entscheidung, Power-Analysis als out-of-scope zu betrachten, basiert auf verschiedenen Faktoren. Zum einen erfordert die Durchführung solcher Angriffe in der Regel physischen Zugang zu den Geräten, was die Bedrohung in vielen realen Szenarien verringert. Zum anderen sind die Implementierungen in sicheren Umgebungen oder speziellen Hardwarevorrichtungen oft gegen solche Angriffe geschützt, sodass die unmittelbare Gefahr in der spezifischen Projektumgebung als gering eingeschätzt wurde.

1.2.4 Wichtigste Positionen des Zahlenmäßigen Nachweises

Die Gesamtförderung betrug 376.633 €. Darin enthalten sind Sachausgaben von 3000 € sowie Reisekosten von 10.000 €.

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 KBLS

Die Entwicklung bei Quantencomputern hat 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 KBLS war, ein geeignetes Verfahren in die Krypto-Bibliothek Botan einzupflegen. Einen besonderen Fokus erhielt dabei die Sicherheit gegen Timing- und Cache-basierte Seitenkanalangriffe. Ferner sollte durch eine gute Usability eine hohe Verbreitung erzielt werden. Dritter Fokus war die Kryptoagilität, um Entwicklern einen einfachen Umstieg von klassischen Verfahren auf Post-Quantum-Verfahren zu ermöglichen, sowie eine hybride Verschlüsselung von klassischen und Post-Quantum-Verfahren.

Erschwert wurde das Projekt durch die Tatsache, dass der Standardisierungsprozess der NIST zu Beginn noch nicht abgeschlossen war und sich weiterhin verzögerte. Der erste große Meilenstein bestand daher aus einer ausführlichen Literaturrecherche und einem systematischen Zusammentragen aller verbliebenen Post-Quantum-Kandidaten der NIST. Dazu wurden von allen Verfahren die relevanten Parameter identifiziert und in einer Datenbank zusammen getragen. Diese Datenbank ist frei zugänglich und ermöglicht Entwicklern über KBLS hinaus eine ausgezeichnete Orientierung, welches der Verfahren für den

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

jeweiligen Anwendungszweck am besten geeignet ist. Diese Datenbank wurde im Verlauf des Projekts mehrfach an den neuesten Stand der Forschung angepasst.

Ein weiteres Arbeitspaket waren ausführliche Entwicklerinterviews, um Bedürfnisse und Wünsche sowie mögliche Hemmnisse von Entwicklern bei der Nutzung von Krypto-Bibliotheken zu ermitteln. Diese hätten im Frühjahr und Sommer 2020 statt finden sollen. Durch die Einschränkungen aufgrund der Corona-Pandemie konnten diese nur verzögert statt finden, wodurch sich auch viele weitere Arbeitspakete nach hinten verschoben.

Für die hybride Verschlüsselung entstanden Konzepte sowohl für Verschlüsselung als auch für Signaturen. Dabei war das Fazit, dass der derzeitige Standard X.509 für Zertifikate durch seine optionalen Felder bereits hybride Signaturen erlaubt.

Größtes Arbeitspaket war die Implementierung von Kyber und Dilithium in die Krypto-Bibliothek Botan, welche von der TU Berlin wissenschaftlich begleitet wurde. Im Laufe des Projekts wurden Seitenkanalangriffe durch Power Analysis bekannt, die im Team intensiv diskutiert wurden. Das abschließende Fazit war, diese als „out of scope“ zu betrachten. Mögliche Timing- und Cache-basierte Seitenkanalangriffe wurden jedoch beachtet, und nach aktuellem wissenschaftlichen Erkenntnisstand ausgeschlossen. Inzwischen sind Kyber und Dilithium in Botan implementiert und bereit für den Einsatz durch weitere Entwickler.