HINWEIS: Frei übersetzt aus dem Englischen. Wir empfehlen als Referenz bei der Bewerbung den englischen Text zu nutzen.

Originaltext auf Englisch finden Sie in folgendem Dokument:

“Horizon Europe Work Programme 2025: Civil Security for Society“
14. Mai 2025 herausgegeben vom ECCC / EU-Kommission

https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/cluster-3-civil-security-society_en?prefLang=de

Förderbereich: Increased Cybersecurity

Förderthema: HORIZON-CL3-2025-02-ECCC-05: Security of implementations of Post-Quantum Cryptography algorithms

Seiten: 103-105

Deutsche Übersetzung des Förderthemas durch das NKCS/ NCC-DE als unterstützendes Informationsangebot erstellt:

HORIZON-CL3-2025-02-ECCC-05: Sicherheit von Implementierungen von Algorithmen der Post-Quantum-Kryptographie

Erwartete Auswirkungen

Vom ECCC eingeleitete Aktion zur Aufnahme der im Abschnitt "Ziel - Erhöhte Cybersicherheit" dieses Teils des Arbeitsprogramms dargelegten Formulierung "erwartete Auswirkungen".

Erwartete Ergebnisse

Es wird erwartet, dass die Ergebnisse der Projekte zu einigen oder allen der folgenden Ergebnisse beitragen:

- Entwurf und Implementierung von Post-Quantum-Kryptographie (PQC)-Algorithmen, die resistent gegen Seitenkanal- und Fehlerangriffe sind;
- Optimierte Gegenmaßnahmen unter Berücksichtigung eines ausgewogenen Verhältnisses zwischen Sicherheit, Leistung und Kosten;
- Empfehlungen für die Implementierung von Gegenmaßnahmen für eine breite Palette von Angriffen, auch unter Angabe der verfügbaren und erforderlichen Hardware;
- Analyse neuer Angriffe oder Angriffskombinationen, die auch durch KI verbessert werden können und auf reale Bedingungen anwendbar sind.
- Entwurf von automatischen Sicherheitsbewertungen für PQC-Implementierungen.

HINWEIS: Frei übersetzt aus dem Englischen. Wir empfehlen als Referenz bei der Bewerbung den englischen Text zu nutzen.

Umfang

Die Sicherheit der Implementierungen von PQC-Algorithmen ist von entscheidender Bedeutung für die Wahrung der Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit digitaler Informationen und Kommunikationen angesichts von Implementierungsangriffen, wie z.B. Seitenkanalangriffen unter Verwendung von Informationen aus dem Timing, dem Stromverbrauch, elektromagnetischer Strahlung, Fehlerangriffen, die den sicheren Betrieb des Geräts stören, und deren Kombination. Solche Angriffe, die möglicherweise durch den Einsatz von Deep Learning noch verstärkt werden, stellen eine erhebliche Bedrohung für (eingebettete und reguläre) Software- und Hardware-Implementierungen dar. In verschiedenen Anwendungsbereichen wie dem Internet der Dinge, Cloud-basierten Anwendungen und der Automobilindustrie führen Maßnahmen zur Verhinderung solcher Angriffe aufgrund der Komplexität der Algorithmen derzeit zu einem erheblichen Ressourcenaufwand, und die Sicherheit bleibt angesichts der begrenzten Erforschung der verschiedenen Angriffsflächen unklar. Gegenmaßnahmen, sofern sie verfügbar sind, können erhebliche Auswirkungen auf die Laufzeit und den Speicherverbrauch haben. Die Resistenz von PQC-Implementierungen gegenüber Implementierungsangriffen ist ein immer häufiger auftretendes Anliegen der Kunden, insbesondere bei der Suche nach dem richtigen Gleichgewicht zwischen Sicherheit und Leistung.

Die Bewertung der Sicherheit von PQC-Algorithmus-Implementierungen gegen Seitenkanal- und Fehlerangriffe ist angesichts der nachgewiesenen Schwachstellen von entscheidender Bedeutung. Verschiedene Gegenmaßnahmen wie Maskierung, Mischen, zufällige Taktung, zufällige Verzögerung, Kodierung mit konstantem Gewicht, Code-Polymorphismus, Kontrollflussintegrität und Neuberechnung kritischer Operationen können eingesetzt werden, um diese Angriffe zu entschärfen. Synergien zwischen spezifischen Gegenmaßnahmen und dem Design kryptographischer Systeme sind für die Prä-Quantum-Kryptographie verfügbar, müssen aber für die Post-Quantum-Kryptographie untersucht werden.

Vorschläge sind willkommen für die Entwicklung von Lösungen, die vor solchen Implementierungsangriffen schützen, und zwar zu vertretbaren Kosten und unter Minimierung der Leistungseinbußen bei gleichzeitiger Aufrechterhaltung der erforderlichen Sicherheit, sowie für die Analyse neuer Angriffe oder Angriffskombinationen, auch durch den Einsatz von KI, für Security-by-Design-Ansätze beim Entwurf von Post-Quantum-Kryptosystemen. Die Aktivitäten können auch zur Entwicklung von Testmethoden und Frameworks für automatisierte Sicherheitsevaluierungen zur Korrektheit und Resistenz gegenüber Remote-Seitenkanalangriffen für reguläre Software und zur Korrektheit und Resistenz gegenüber einer breiten Palette von Implementierungsangriffen für eingebettete Software und Hardware führen.

Art der Maßnahme	Research and Innovation Actions
Vorläufiges Budget	*6 Mio. EUR*
Vorläufiges Budget pro Projekt	*2-3 Mio. EUR*
Zuwendungsberechtigt	Rechtsträger mit Sitz in EU-Mitgliedstaaten und assoziierten Länder, die nicht direkt oder indirekt von Drittländern kontrolliert werden
Abrechnung	Förderfähige Kosten werden als Lump Sums (Pauschalbeträge) gewährt
Sicherheit	Einige Aktivitäten, die sich aus diesem Thema ergeben, können die Verwendung von als Verschlusssache eingestuften Hintergrundinformationen und/oder die Erstellung von sicherheitsempfindlichen Ergebnissen (EU-

HINWEIS: Frei übersetzt aus dem Englischen. Wir empfehlen als Referenz bei der Bewerbung den englischen Text zu nutzen.

	Verschlusssachen und SEN) beinhalten. Bitte beachten Sie die entsprechenden Bestimmungen in Abschnitt B Sicherheit - EU-Verschlusssachen und sensible Informationen der Allgemeinen Anhänge.

Das **Nationale Koordinierungszentrum für Cybersicherheit (NKCS/ NCC-DE)**

berät zu **EU-Fördermöglichkeiten in der Cybersicherheit**

und hilft bei der **Vernetzung mit EU-Partnern**.

Sie erreichen uns unter **nkcs@bsi.bund.de**