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-04: Security evaluations of Post-Quantum Cryptography (PQC) primitives

Seiten: 101-103

---

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

# HORIZON-CL3-2025-02-ECCC-04: Sicherheitsbewertung von Post-Quantum-Kryptographie-Primitiven

## 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:

- Durchbrüche beim Verständnis der Quantenhärte verschiedener mathematischer Problemklassen, die die Sicherheit aktueller und zukünftiger Post-Quantum-Kryptosysteme untermauern;
- Neue Quantenalgorithmen mit signifikanter Quantenbeschleunigung für gitterbasierte, codebasierte und möglicherweise andere mathematische Problemklassen;
- Verbesserte Implementierung von Quantenalgorithmen unter Verwendung von High-Level-Quantenprogrammiersprachen zur Lösung mathematischer Probleme, die den Kern von Kryptosystemen bilden;
- Einrichtung von Umgebungen, in denen die Robustheit von Kryptosystemen gegenüber Quantenangreifern getestet wird;

- KI-basierte Ansätze, die bei der Entdeckung von Schwachstellen in gitterbasierten oder anderen mathematischen Problemklassen helfen;
- Ergebnisse der Kryptoanalyse;
- Parameter-Vorschläge zur Schaffung eines robusten Satzes kryptographischer Bausteine für die Post-Quantum-Cybersicherheit und das Design von Post-Quantum-Kryptosystemen mit verbesserter Sicherheit gegen Quanten- oder KI-basierte Angriffe.

## Umfang

Die intrinsische Sicherheit von PQC-Algorithmen basiert auf mathematischen Problemen, die sowohl für klassische als auch für Quantencomputer als unlösbar angesehen werden. Die Bewertung der Quantensicherheit von Post-Quantum-Primitiven ist von grundlegender Bedeutung, um unser Vertrauen in Post-Quantum-Kryptosysteme zu stärken. Die Entwicklung von Quantenalgorithmen, die eine signifikante Quantenbeschleunigung aufweisen, wäre ein großer Durchbruch, der eine Neubewertung der Sicherheit von Kryptosystemen (gitterbasiert, codebasiert und andere) erforderlich machen würde. Wird hingegen keine signifikante Quantenbeschleunigung entdeckt, würde dies unser Vertrauen in die Sicherheit dieser Post-Quanten-Kryptosysteme stärken, auch wenn einige Parameter möglicherweise noch einer Feinabstimmung bedürfen. Außerdem wurden die bestehenden Quantenangriffe bisher hauptsächlich theoretisch analysiert. Ihre Anwendung auf heutige Kryptosysteme scheitert jedoch an einem Mangel an effizienten Implementierungen und Hardware. Es sind auch Studien zu KI-basierten Ansätzen erforderlich, mit denen bestimmte Schemata bei bestimmten Implementierungsentscheidungen angegriffen werden können. Die Entdeckung möglicher Schwachstellen kann der Forschungsgemeinschaft helfen, robustere Post-Quantum-Kryptosysteme zu entwickeln.

Vorschläge zur Bewertung der Sicherheit von Post-Quantum-Primitiven durch Studien, die sich auf mögliche Quantenalgorithmen mit nachweislicher Geschwindigkeitssteigerung, eventuell auch in Kombination mit KI, oder auf ausschließlich KI-basierte Ansätze konzentrieren, sind willkommen. Die Sicherheit von gitter- und kodebasierten PQC-Algorithmen könnte im Vordergrund stehen, aber auch andere mathematische Problemklassen sind nicht ausgeschlossen. Da die beispiellose Rechenleistung von Quantencomputern die KI-Fähigkeiten erheblich verbessern kann, kann auch eine Kombination verschiedener Ansätze in Betracht gezogen werden. Konsortien mit Bewerbern, die über Erfahrungen in der Post-Quantum-Kryptographie und im Quantencomputing verfügen, werden besonders gefördert. Die Projekte sollten zur Identifizierung von Schwachstellen aktueller kryptographischer Post-Quantum-Bausteine und zu praktischen Empfehlungen für Parameter für die Entwicklung von Post-Quantum-Kryptosystemen mit verbesserter Sicherheit gegen Quantenangriffe und zukünftige Fortschritte beim Code-Breaking und der KI führen.

| | |
|---|---|
| Art der Maßnahme | Research and Innovation Actions |
| Vorläufiges Budget | *4 Mio. EUR* |
| Vorläufiges Budget pro Projekt | *2-3 Mio. EUR* |
| Ausschreibungsstart | 12.06.2025 |
| Zuwendungsberechtigt | Rechtsträger mit Sitz in EU-Mitgliedstaaten, assoziierten Ländern und OECD-Ländern, 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 |

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

| | |
|---|---|
| | eingestuften Hintergrundinformationen und/oder die Erstellung von sicherheitsempfindlichen Ergebnissen (EU-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**