Sicherheitsbewertung von Post-Quantum-Kryptographie-Primitiven

HORIZON-CL3-2025-02-CS-04: Security evaluation of Post-Quantum Cryptography (PQC) primitives

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

1

Für dieses Topic aus **Horizont Europa 2025** beträgt das Fördervolumen insgesamt **4 Mio. €** und wird vom ECCC initiiert. Die vorgesehene Projektgröße liegt zwischen 2 und 3 Mio. €.

2

Art der Maßnahme: Research and Innovation Actions
Förderquote: 100 %
Ausschreibungsstart: 12. Juni 2025
Einreichungsfrist: 12. November 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

Erwartete Ergebnisse

Geförderte Projekte entwickeln innovative Lösungen zur Stärkung kryptografischer Sicherheit – darunter KI-gestützte Schwachstellenerkennung, beschleunigte Quantenalgorithmen (z. B. für gitterbasierte Probleme) und optimierte Implementierungen mit Quantenprogrammiersprachen. Ziel sind Testumgebungen zur Quantenresistenz-Bewertung, verbesserte Kryptoanalyse sowie robuste Post-Quantum-Kryptosysteme, die gleichzeitig gegen Quanten- und KI-Angriffe geschützt sind.

Umfang

Im Fokus stehen mathematische Sicherheitsanalysen von Post-Quantum-Systemen, Risikobewertungen von Quantenangriffen und KI-gestützte Angriffssimulationen auf PQC-Implementierungen. Untersucht wird, wie Quantencomputer KI-Angriffe beschleunigen und welche Schutzmaßnahmen neue Bedrohungsszenarien abwehren können.

NKCS
NATIONALES KOORDINIERUNGSZENTRUM FÜR CYBERSICHERHEIT
DEUTSCHLAND

Sie haben Fragen? Nehmen Sie Kontakt mit uns auf:
www.nkcs.bund.de/de/kontakt