# Aktuelle Fortschritte und Anstrengungen bei Post-Quanten-Kryptoverfahren

**Vorschlag für einen Beitrag zur Konferenz CODE2018**

Alexander von Gernler
Leiter der Forschung, genua GmbH

4. Mai 2018

## 1 Inhalt

Der beabsichtigte Beitrag fasst die Fortschritte im Bereich praxistauglicher Post-Quanten-Kryptographie (PQC)-Verfahren der letzten beiden Jahre aus Sicht der genua-Forschung zusammen. Zunächst wird das Thema mit einer kurzen Rekapitulation der allgemeinen PQC-Ausgangssituation motiviert.

Hervorzuheben sind zum einen der bereits in der finalen Phase der Standardisierung zum Internet-RFC befindliche hashbasierte PQC-Signaturalgorithmus *XMSS MT*[1]. Das Unternehmen hat hier in Kooperation mit der TU Darmstadt ein erfolgreiches Forschungsprojekt zur Nutzbarmachung des Algorithmus betrieben. Die dort erarbeiteten Signaturverfahren sind bereits in den Produkten der Firma aktiv und schützen dort die Software-Updates der Firewall-Produkte.

Zum anderen soll die Sprache auf laufende Arbeiten zur Etablierung PQC-sicher verschlüsselter VPN-Strecken kommen. Da es sich hier um aktuell ausgeführte Forschung handelt, besteht der zweite Teil aus der Formulierung der Problemstellung sowie der Präsentation vielversprechender Ansätze.

## 2 Rahmendaten

**Zugrundeliegende Technologie:** Post-Quanten-Kryptographie

**Reifegrade:** Signaturverfahrenen nahe finalem Standard und bereits im Einsatz. Verschlüsselung in Erforschung.

[1] https://datatracker.ietf.org/doc/draft-irtf-cfrg-xmss-hash-based-signatures/