Kuriose Nachrichten

Beitrag von „Seph“ vom 6. September 2025 09:00

> Zitat von Moebius
>
> Quantencomputer sind ein grundsätzlicher Gamechanger bei der Verwendung von Passwörtern (die damit entschlüsselt werden können) und der Generierung echter Zufallszahlen (dafür werden sie bereits verwendet, weil ein einziges qubit dafür im Prinzip reicht, so weit ist man längst)

Und selbst das ist derzeit noch weniger kritisch, als gemeinhin angenommen wird. Der häufig verwendete Standard AES-256 ist voraussichtlich quantensicher - ähnlich wie die Hash-Algorithmen SHA-384 und SHA-512. Es gibt zwar einen Algorithmus, der die Komplexität eines Angriffs auf symmetrische Verschlüsselungsverfahren spürbar reduzieren kann, diese aber nicht aushebelt. Inwiefern dieser Algorithmus überhaupt praktisch realisierbar ist, ist auch noch offen.

Größere Sorgen muss man sich um asymmetrische Verfahren machen, aber auch da ist man von einer praktischen Implentierung noch ein gutes Stück weg, da real existierende Quantencomputer schlicht noch zu viele Fehler machen und dementsprechend die benötigte Menge an Qubits für den Algorithmus stark ansteigen.