Kuriose Nachrichten

Beitrag von „Volker_D“ vom 7. September 2025 22:55

> Zitat von Seph
>
> Dann noch einmal: es ging nicht um die Reduktion von 128 Bit auf 64 Bit, die durchaus kritisch ist, sondern um die Reduktion von 256 Bit auf 128 Bit, die alles andere als kritisch ist. Derzeitiger Goldstandard bei symmetrischen Verfahren ist der AES-256, dessen Sicherheit in der Praxis aber auch bei erfolgreicher Implementierung von Grovers Algorithmus auf Quantencomputern noch hinreichend gewährleistet wäre.

Das macht es doch nur schlimmer. Wenn es durch den Gover Algorithmus von 2^256 auf 2^128 halbiert wird und vorher 10^10 Jahre benötigt hat, dann sind es danach nur noch 10^-21 Sekunden. Also sofort. Setzt aber einen Quantencomputer mit sehr vielen Qbit vorraus. siehe #607