# Kuriose Nachrichten

## Beitrag von „Seph“ vom 7. September 2025 22:07

> Zitat von Volker_D
>
> Also gut, dann genauer gerechnet.
>
> Wenn sich die Komplexität von 2^128 auf 2^64 halbiert und mal angenommen du brauchst vorher 10^10 Jahre zum knacken, dann dauert es danach nur noch 0,02 Sekunden.

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.

Dass diese Halbierung der Schlüssellänge eine extreme Reduktion der Komplexität eines Angriffs bedeutet, ist allen halbwegs matheaffinen Personen sofort klar. Nur ergibt sich daraus in der Praxis noch nicht die vielbeschworene Nutzlosigkeit bisheriger (symmetrischer) Verschlüsselungsverfahren.

Die von dir zitierten Zahlen mögen geeignet sein, um diese extreme Reduktion der Komplexität zu verdeutlichen. Sie bilden aber nicht die tatsächlich benötigte Zeit für einen Angriff auf AES-256 ab...auch nicht unter Berücksichtigung der theoretischen Möglichkeiten von Grovers Algorithmus auf derzeit noch nicht existenten genügend "großen" Quantencomputern.