Kuriose Nachrichten

Beitrag von „Seph“ vom 7. September 2025 19:14

> Zitat von Volker_D
>
> Mal Überschlagen:
>
> 2^256 = 1,1E77
>
> 2^128= 3,8E38
>
> Ok, dass ist jetzt nicht zu O(1) geworden, aber wenn es also vorher 10000 Jahre zum Knack gebraucht hat, dann wird dann danach weniger als 1 Sekunde benötigt. Da würde ich schon von "brechen" sprechen.

Nur dauerte es vorher nicht nur 10000 Jahre. Ein Brute-Force-Angriff auf "nur noch AES-128" liegt im Zeitbedarf noch immer um Größenordnungen über dem Alter des Universums. Mir treibt die effektive Halbierung der Schlüssellänge bei symmetrischen Verfahren durch Grover´s Algorithmus jedenfalls in der Praxis keinen Angstschweiß auf die Stirn, auch wenn diese natürlich bemerkenswert ist und für sehr kurze Schlüssel tatsächlich ein Problem darstellen kann. Das bekommt man bei den symmetrischen Verfahren aber durch angepasste Schlüssellängen ganz gut in den Griff.