

Kuriose Nachrichten

Beitrag von „Volker_D“ vom 6. September 2025 10:37

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.

Hauptproblem ist aber, dass da ein Rechner mit 128 Qbit nicht ausreicht. Dafür sollen wohl schätzungsweise einige hundert tausend QBits benötigt werden.