Kuriose Nachrichten

Beitrag von „Volker_D“ vom 6. September 2025 10:11

> Zitat von Seph
>
> Von dem sprach ich. Dieser reduziert die Komplexität zwar erheblich, aber bricht die Verfahren deswegen noch lange nicht. Zudem ist eine praktische Umsetzung von Grover´s Algorithmus derzeit noch nicht absehbar.

Wenn ich es richtig im Kopf habe, dann reduziert er bei AES-256 Komplexität von 2^256 auf 2^128.

Grover ist aber schon 2017 von IBM auf einem 5-Qubit-Systemen umgesetzt worden. Das ist aber viel zu wenig "Speicherplatz" um AES-256 anzugreifen. Dafür werden größere Quantencomputer benötigt. Das wird aber, so wette ich, in den nächsten 20 Jahren nichts.