

Kuriose Nachrichten

Beitrag von „Seph“ vom 6. September 2025 09:56

[Zitat von Volker D](#)

Der AES und SHA Algorithmus lässt sich von Quantencomputer mit dem Grover's Algorithmus angreifen.

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.