Kuriose Nachrichten

Beitrag von „Volker_D“ vom 6. September 2025 09:36

Jain. AES(-256) und SHA(-512) sind nicht voll quantensicher.

Nur unter den im Moment zu erwartenden Quantencomputer der nächsten Jahre (was auch immer damit gemeint ist) wird dieses angenommen.

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

Das BSI stuft AES als nicht quantensicher ein.

Das ist aber nicht all zu wild, da a) es noch relativ lange dauern wird, bis es Quantencomputer gibt, die es können und b) schon alternative Algorithmen zur Verfügung stehen.