

Is cryptography dead?

Imagine:

15 years from now
someone announces
successful construction
of a large quantum computer.

New York Times headline:

**“INTERNET CRYPTOGRAPHY
KILLED BY PHYSICISTS.”**

Users panic.

What happens to cryptography?

RSA: Dead.

DSA: Dead.

ECDSA: Dead.

ECC in general: Dead.

HECC in general: Dead.

Buchmann–Williams: Dead.

Class groups in general: Dead.

“They’re all dead, Dave.”