

Quantum computing is coming: Are you quantum-security ready?

SAN DIEGO, CA, UNITED STATES, January 8, 2021 /EINPresswire.com/ --

In today's digital economy, data are the new 'currency'. Data drive interactions between individuals, organizations, and governments. They empower decision-making and problem-solving processes, support positive change, and provide direction toward operational efficiency, productivity, and profitability. Data are also used as 'weapons' in performing mass surveillance, espionage, cyberattacks, and political interferences.

For now, asymmetric public-key encryption systems, like that of Rivest-Shamir-Adleman's (RSA), can barely protect the world's data from bad actors, being a relatively slow algorithm and one of the oldest cryptosystems. Moreover, as the world waits for quantum computers that will be accessible and commercially available, organizations and governments everywhere must prepare for a harsher reality: current cryptographic defenses that are supposed to secure their data will not be against these bad actors.

Cryptography methods that safeguard the world's data — from financial and health information to passwords, digital signatures, and top-secret military communications — are based on some mathematical problems that would take classical computers ages to solve (up to billions of years).

This is not so for quantum computers. Once a sufficiently powerful quantum computer becomes commercially available, these cryptographic defenses will collapse very quickly. The US National Academies of Sciences, Engineering, and Medicine predicts that a powerful quantum computer with around 2,300 qubits could crack an RSA 1024 encryption in less than a day.

Quantum computing is becoming a threat to traditional encryption!

Without strong, quantum-safe cryptography, bad actors with access to quantum computers can target data that power all kinds of modern applications. Vadim Lyubashevsky, a cryptography researcher with IBM, completely agrees, claiming that "somebody could be harvesting the data now" so they could "decrypt them later". Alarming, this means that hackers are already collecting or stealing data from businesses and governments while waiting for a quantum computer to become available. Once it is available, they can use it to decrypt the previously encrypted sensitive data for malicious purposes.

Businesses and governments must take action as soon as possible to protect their data now. They must define their 'data storage' timeline to figure out which data will just be around for a few years, versus which data will retain value for at least thirty years. Simply put, they must start thinking about quantum-proof cryptography methods sooner, rather than later, if they do not want to be sorry.

Are you quantum-security ready?

The author would like to thank [Quantropi](#), Inc., of Ottawa, Canada for insightful discussions about internet communication security. Quantropi is a quantum communications company that provides the world's first non-photon quantum key distribution over the Internet.

About the Author: Ken Kuang is a successful business owner, seasoned executive and innovator. He founded [Torrey Hills Technologies, LLC](#) in 2004. From 2004-2013, he led Torrey Hills to rank #188 in INC500 Fast Growing Private Companies in America and rank #2 in San Diego Business Journal 100 Fastest-Growing Private Companies in San Diego and was the finalist for the Most Admired CEO's three times in San Diego. Ken is recognized as an industry expert in RF/MW packaging, has presented many times in packaging conferences, and won the Best Session Paper in IMAPS 2000, Best Symposium Paper in ICEPT 2003, the IMAPS President Awards in 2008 & 2012, and Fellow of the Society in 2014. His company received the 2013 Tibbetts Award at the White House on May 16, 2013, and was cited for Excellence in Small Business Innovation Research.

Ken Kuang
Torrey Hills Technologies, LLC
8585586666
[email us here](#)

Visit us on social media:

[Facebook](#)
[Twitter](#)
[LinkedIn](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/534237834>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2021 IPD Group, Inc. All Right Reserved.