# Quantum Resistance and the Internet of Things

Charles W. Clark
Joint Quantum Institute, National Institute of Standards and Technology and the University of Maryland
ScienceCast, Inc.

A specter is haunting cybersecurity - the specter of quantum computing.

We live in a Web 2.0 world, with 7 billion smartphones and an emerging Internet of Things (IoT), in which distributed computing and communication are pervasive. Security of this interconnected network depends upon public key infrastructure (PKI). Largely unnoticed by the world's users, each day PKI secures an exabyte of internet traffic, related to transfer of governmental, financial, industrial, medical, commercial and other information. A most consequential development of mathematics and computer science [1], PKI security derives from asymmetric complexity. It can scramble a message far more efficiently than any known technique of unscrambling. All internet messages appear at first glance to be random, until they are decoded with the appropriate key.

In 1994, [2] Peter Shor showed that quantum physics, of all things, exposes PKI to efficient cryptanalytic attack. No quantum machine has yet attained sufficient power to do this, but the enabling technology is developing rapidly.

What a good time for a brief tutorial on classical and quantum logic, machines, cryptography, computation and fundamental order and randomness!

[1] A. M. Turing Awards for 2002 and 2015: https://amturing.acm.org/byyear.cfm
[2] "The Early Days of Quantum Computation," P. W. Shor, arXiv:2208.09964 (2022)