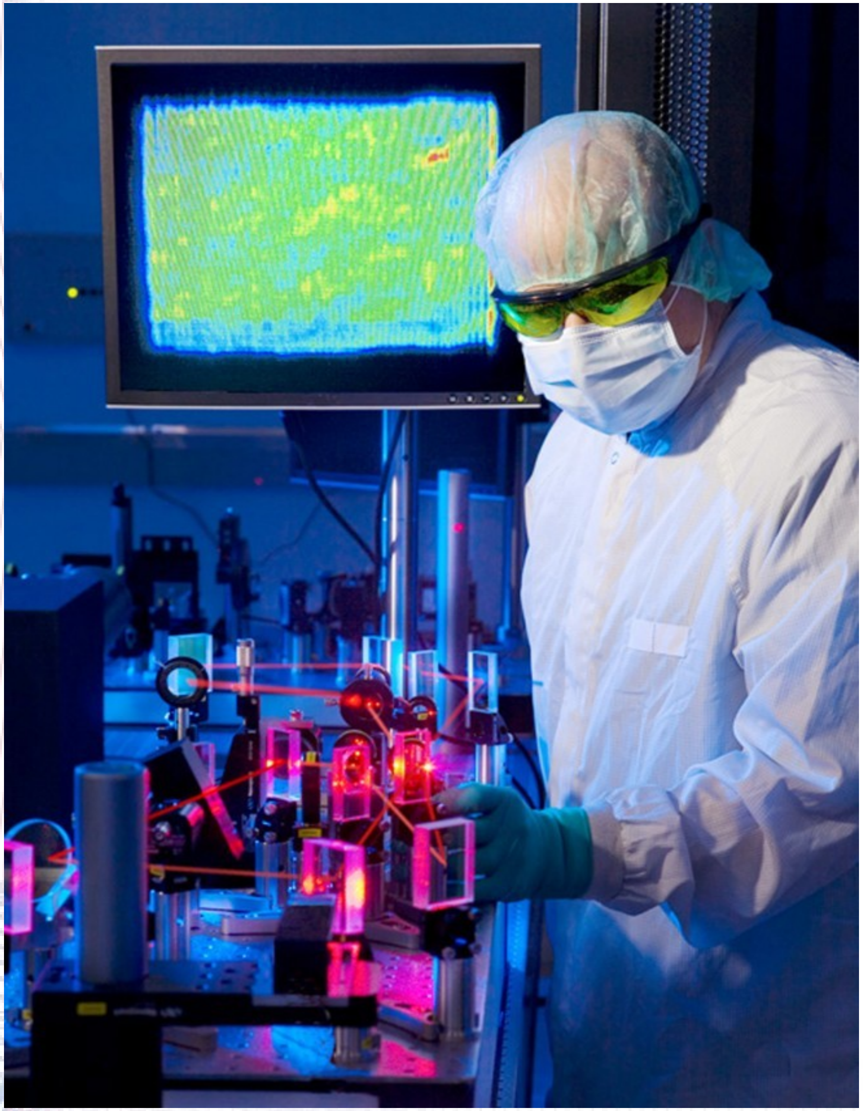
Quantum Computing



How the Advent of Quantum Computing Will Change Encryption

Encryption Arms Race

- DES-56 was adopted in 1977. It was cracked by the DESCHALL Project in 1997 using 78,000 computers. It took 96 days.
- PGP released in 1991 based on RSA-129. RSA-129 cracked in 1994 by volunteers organized by Paul Leyland at Oxford. It took 600 computers 6 months.
- PKCS1 released in 1991 used in SSL. Cracked by researchers in Bell Labs in 1998.
- MD5 released in 1991. Collisions found by researchers from Shandong University in Aug 2004.
- SHA-1 released 1995. Collisions found by researchers from Shandong University in Feb 2005.

- CSS released in 1996. Cracked by Jon Lech Johansen in 1999 using a single computer.
- WEP released in 1997. RC4 cipher used in WEP cracked by Adi Shamir in 2001 using a single computer.
- AES adopted as new standard in 2001. Not cracked yet...
- July 2002 Distributed computing effort based in Austin TX Distributed.net cracked RC5-64. It took 4 years and over 300,000 computers
- Dec 2009 RSA-768 was cracked by a collection of cryptography researchers including Phil Zimmerman. It took 2 years and 200 computers.
- Dec 2009 members of Chaos Computer Club in Germany compiled 2Tb of rainbow tables capable of realtime decrypting GSM A5/1 used for cell phones

Noticing a pattern?

Encryption ciphers generally last about 10 years give or take.

After one is cracked or expected to be cracked a new one is devised.

The replacement cipher will have more bits and take more processing power to crack.

Quantum Computers

1981 Richard Feynman proposed the idea of using particles exhibiting quantum properties as the basis for a new type of computer

1994 Peter Shor devised an algorithm which would utilize the special properties of the then theoretical quantum computer known as probability wave cancellation to rapidly factor large numbers.

1996 Lov Grover devised an algorithm to utilize special properties of a quantum computer to search a database exponentially faster than could be done using a classic computer.

1998 First quantum computer created using 2 qubits by Isaac Chuang of UC Berkley

1999 First functioning quantum logic gate created by researchers at Notre Dame.

2001 Shor's Algorithm run on a 7 qubit quantum computer by researchers at IBM.

2004 A joint research effort by Duke and Purdue University created the first stable quantum transistor using 2 quantum dots connected by 8 logic gates.

2005 Physicists at GIT create quantum memory capable of transmitting and storing quantum information.

2006 Scientists at University of Chicago demonstrate Zeno Effect to analyze the results of a computation on a quantum computer prior to the computation having been run.

2007 Quantum data bus allowing communication between remote qubits created by scientists at Yale University.

2008 Scientists from a consortium of international universities create a quantum “hard drive” using the nucleus of a phosphorus atom allowing long term storage of quantum information.

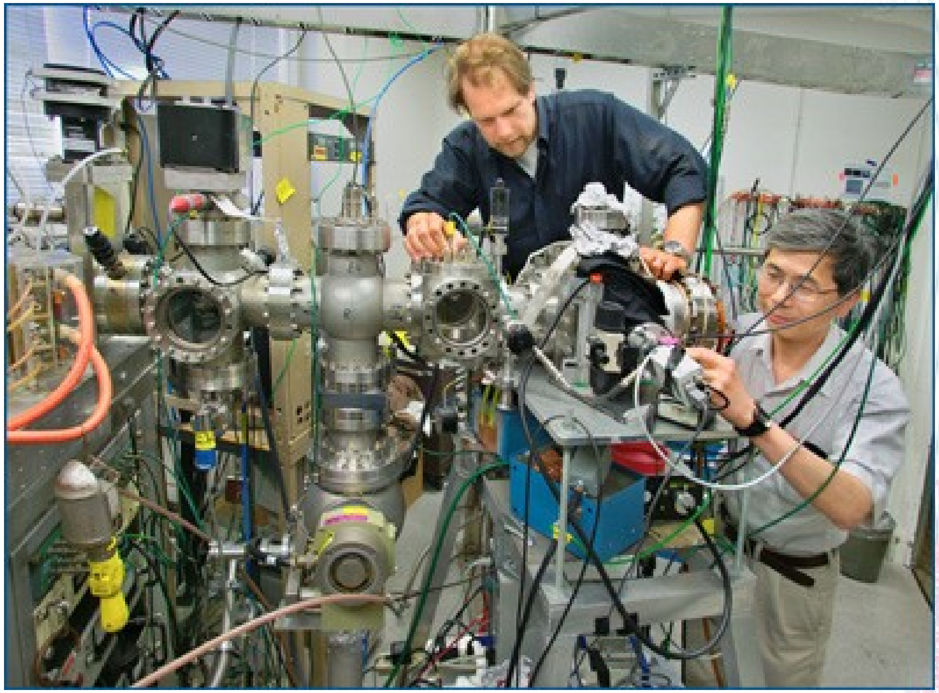
Feb 2009 Quantum data buffering demonstrated by researchers at NIST and University of Maryland.

June 2009 First quantum computer using solid state electronics created by researchers at Yale.

Dec 2009 Researchers at Google develop new quantum algorithm for search that can identify the subject of photographs.

Current State of Quantum Computing

- All the basic computing components have been created: CPU, bus, memory, hard drive.
- All the major technical obstacles have been solved or are nearly solved:
- Input/output
- Storing/retrieving quantum data
- Error correction
- Decoherence
- Isolation from interference



Quantum computers are really good at certain tasks.

-Factoring large numbers
-Searching a database

Q: What kinds of encryption relies on the difficulty of factoring large numbers?

Asymmetric ciphers are in widespread use on the internet because you can share your public key without jeopardizing your private key.

They are used for:

- email encryption PGP/GPG
- certificate stores X.509
- secure web communications SSL/TLS
- data in motion

Symmetric ciphers are used for data at rest ie AES, Blowfish, etc

Technologies based on vulnerable ciphers include:

- IKE
- IPSEC
- SSH
- Smart Cards
- SILC
- ZRTP
- S/MIME
- EAP
- LDAP
- SSL

Presently quantum computers are no more than pocket calculators, but once they reach the supercomputer stage, all those ciphers and protocols are toast!

It would take a classical computer 10 million billion billion years to factor a 1000 digit number.

A quantum computer could do it in 40 minutes.[1]

[1] Department of Computing, Department of Electrical and Electronic Engineering, Imperial College of Science Technology and Medicine, Journal 1997 Vol 4

What does it mean?

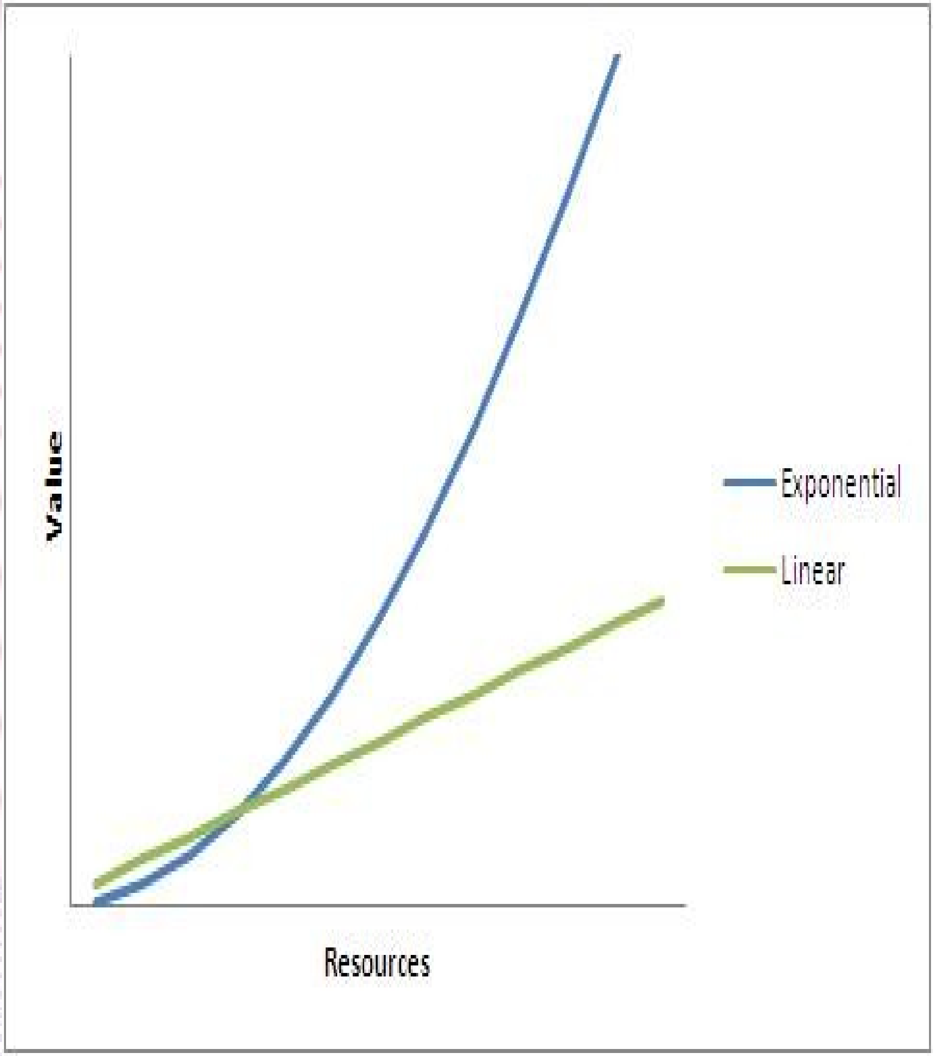
Truly secure Internet communication will no longer be possible.

Previously stored communications will be able to be deciphered.

- Personal secrets
- Trade secrets
- Military secrets

Can't we just come up with better encryption algorithms or longer keys?

The Future



Moore's Law describes linear advancement of computer power.

Quantum Computers are predicted to grow in power exponentially.

Moore's Law is predicted to end in 2020 when transistors reach atomic size and become subject to the laws of quantum physics.

Classical computing will stagnate as quantum computers take off!

Supercomputers

A supercomputer used to be defined as a computer capable of a teraflop or 1 trillion floating point operations per second.

Recent advances have redefined a supercomputer as being capable of a petaflop or 1 quadrillion flops.

The fastest single supercomputer today is the Cray XT5 Jaguar at the Oak Ridge National Laboratory capable of 1.759 Pflops

Clusters of normal computers can be considered quasi-supercomputers. The fastest of these Folding @ home is capable of 7.8 Pflops

Quantum Supercomputers are expected to be measured in Exaflops initially and eventually in Zetaflops.

An Exaflop is 1 million teraflops

A Zetaflop is 1 million petaflops

Some things an Exaflop supercomputer could do – modeling the movements of all the atoms in a fusion reaction.

Some things a Zetaflop computer could do – simulate the entire global climate in real time!

Computers at this scale will also be able to defeat current symmetric encryption.

Efficient collision finding algorithm?

Computer Revolution all over again

Complex and cost prohibitive materials (cryogenic cooling, diamond nano-wire, powerful lasers, etc) will prevent personal quantum computers for foreseeable future.

Only encryption capable of surviving will be quantum encryption because it doesn't depend on complex math to protect information.

Questions or Comments

Brian Milliron
ECR Security
Brian@ECRSecurity.com