Introduction to Quantum Computing & Quantum Cryptography

Jonathan P. Dowling

Co-Director, Hearne Institute for Theoretical Physics
Louisiana State University, Baton Rouge, Louisiana USA
http://quantum.phys.lsu.edu

&

建道灵
Associate Member
Computational Science Research Center
Beijing, China
http://csrc.ac.cn/
PUBLIC KEY SECRET CODES ON THE INTERNET

1. Sender encrypts message using receiver’s public key. Anyone who knows receiver’s public key can do this.

2. Receiver decrypts the message using his private key, which only he knows.

These secret codes protect your credit card information!
Making a Secret Code is as Easy as Multiplication:
15,485,863 • 32,452,843 = 502,560,280,685,509
Breaking a Secret Code is as Hard as Factoring:

\[ 502,560,280,658,509 = 15,485,863 \cdot 32,452,843 \]
FACTORING BIG NUMBERS IS **VERY HARD!**

If every particle in the Universe was a **classical** computer running at full speed for the entire life of the Universe (about 12 billion years) that would be still insufficient to factor a 2,000 digit number.

Current Internet Encryption Uses 1,000 Digit Numbers.

Your Credit Card Number Is Safe!

Or Is It???
CRACKING THE CODE: LIFE IMITATES ART

Quantum Computer Can Factor a 2,000 Digit Number In Less Than a Second!
A Car’s Odometer is Like a Classical Computer Register: It Shows Only One Six-Digit Number at a Time.
A Quantum Odometer Can Store 999,999 Six-Digit Numbers at One Time!
REALITY: National Institute of Standards and Technology

SMALL QUANTUM COMPUTER RUNS AN ATOMIC CLOCK
WE DESIGN QUANTUM COMPUTER CHIPS
QUANTUM CRYPTOGRAPHY

When Quantum Computers Come Online What Will Keep Our Credit Cards Safe on the Internet?

Quantum Cryptography!
ONE-TIME PAD  PRIVATE SECRET KEY SYSTEM

Secret Code Invented by G.S. Vernan — An Army Telegraph Officer During the Civil War.

Proven Unbreakable by Claude Shannon at Bell Labs in the 1940’s.

Unbreakable by Even A Quantum Computer!
ALICE SENDS A COPY OF THE KEY TO BOB

Problem: Eavesdropper Can Always Make a Copy of the Pad!
ALICE SENDS A COPY OF THE KEY TO BOB

Problem: Eavesdropper Can Always Make a Copy of the Pad!
EVE CAN’T COPY A QUANTUM PAD!

Optics

Electronic Control Board

quantum channel (optical fiber 87km, approx. 54 miles)

Optics

photon detector

Electronic Control Board

QST
HOW DOES A QUANTUM CRYPTO WORK?

In Classical Fiber Optics Networks Eve Can Always Steal a Little of the Light and Make a Copy of the Key.
EVE CAN’T COPY A QUANTUM PHOTON WITHOUT DESTROYING THE INFORMATION
YOU CAN BUY A QUANTUM CRYPTO SYSTEM!
THE QUANTUM INTERNET IS HERE!

Canary Islands

Switzerland

Boston
THE QUANTUM SKYNET IS ALSO HERE!

In 2008 — Austrian Scientists Transmitted Single Photons to a Japanese Communications Satellite and Back.

Americans Have a Similar Project — The Goal is To Provide SECRET CODES for US Satellites.
LSU DESIGNS ROUTERS FOR THE QUANTUM INTERNET AND MODELS ATMOSPHERIC TRANSMISSION FOR SKYNET