Title: Public Lecture = Mike Mosca

Date: Oct 05, 2016 02:25 PM

URL: http://pirsa.org/16100059

Abstract:

As We Enter the New Quantum Era

Perimeter Institute Public Lecture

Michele Mosca

5 October 2016

CryptoWorks21

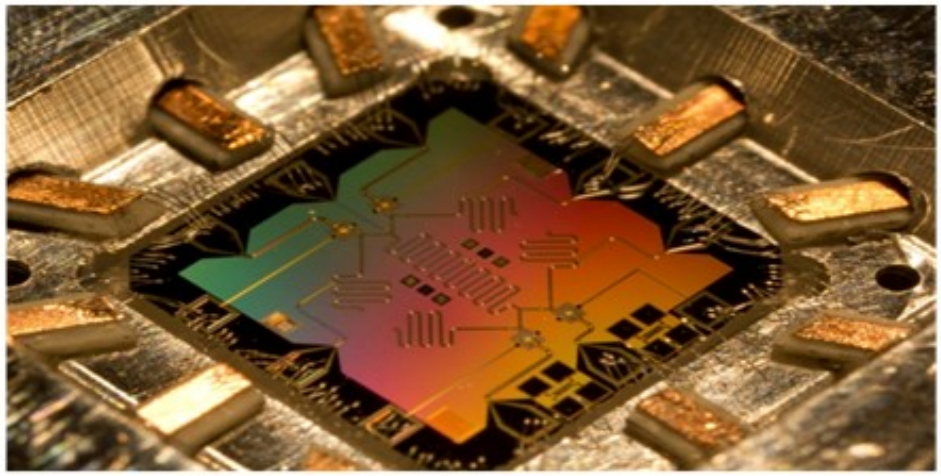
evolution

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

PERIMETER PI INSTITUTE FOR THEORETICAL PHYSICS

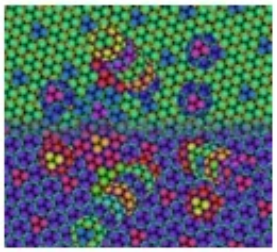
A new paradigm for physics: quantum mechanics

A new paradigm for computation: quantum computation

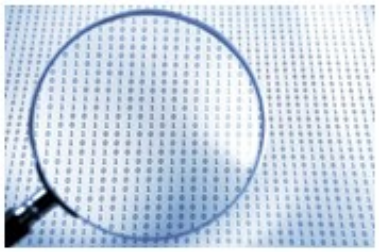


E. Lucero, D. Mariantoni, and M. Mariantoni

New paradigm brings new possibilities



Designing new materials, drugs, etc.



Optimizing

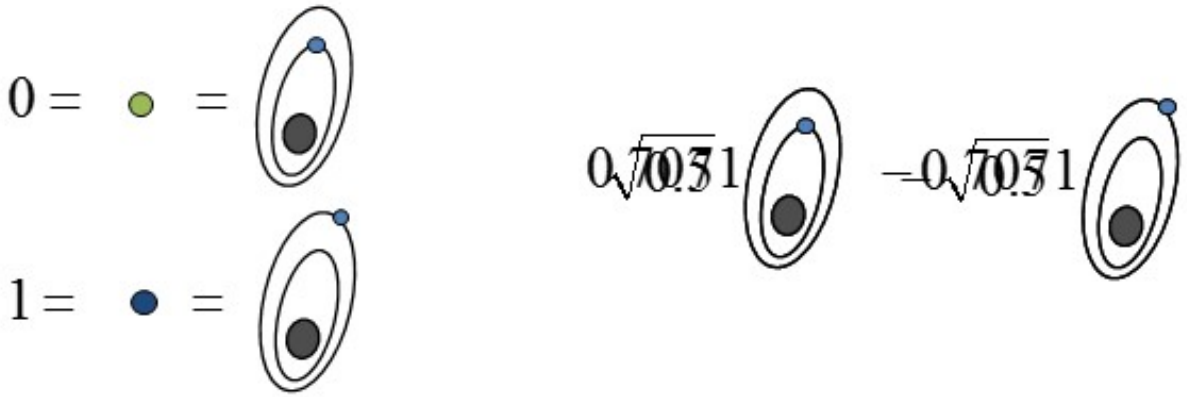
Sensing and measuring

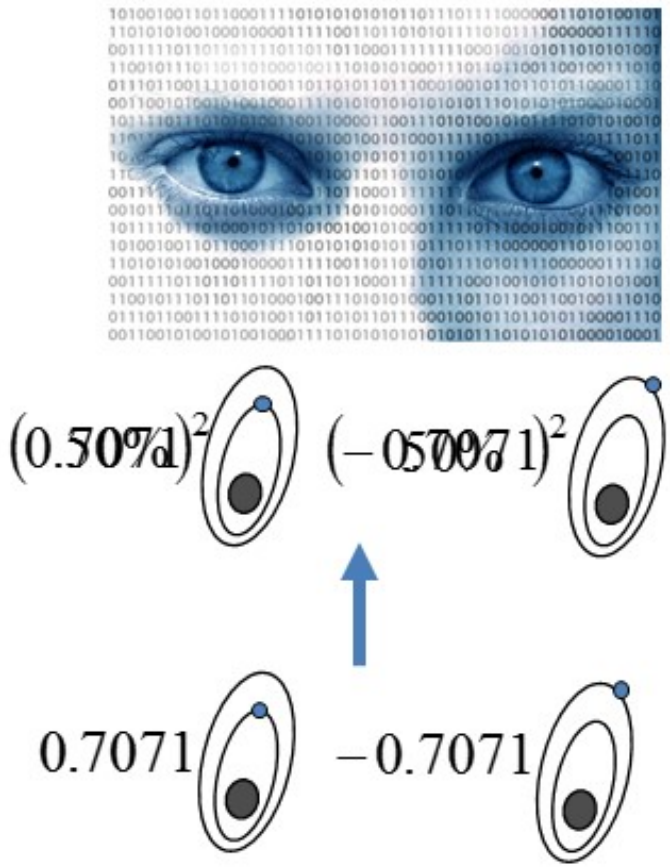
Secure communication

What else???

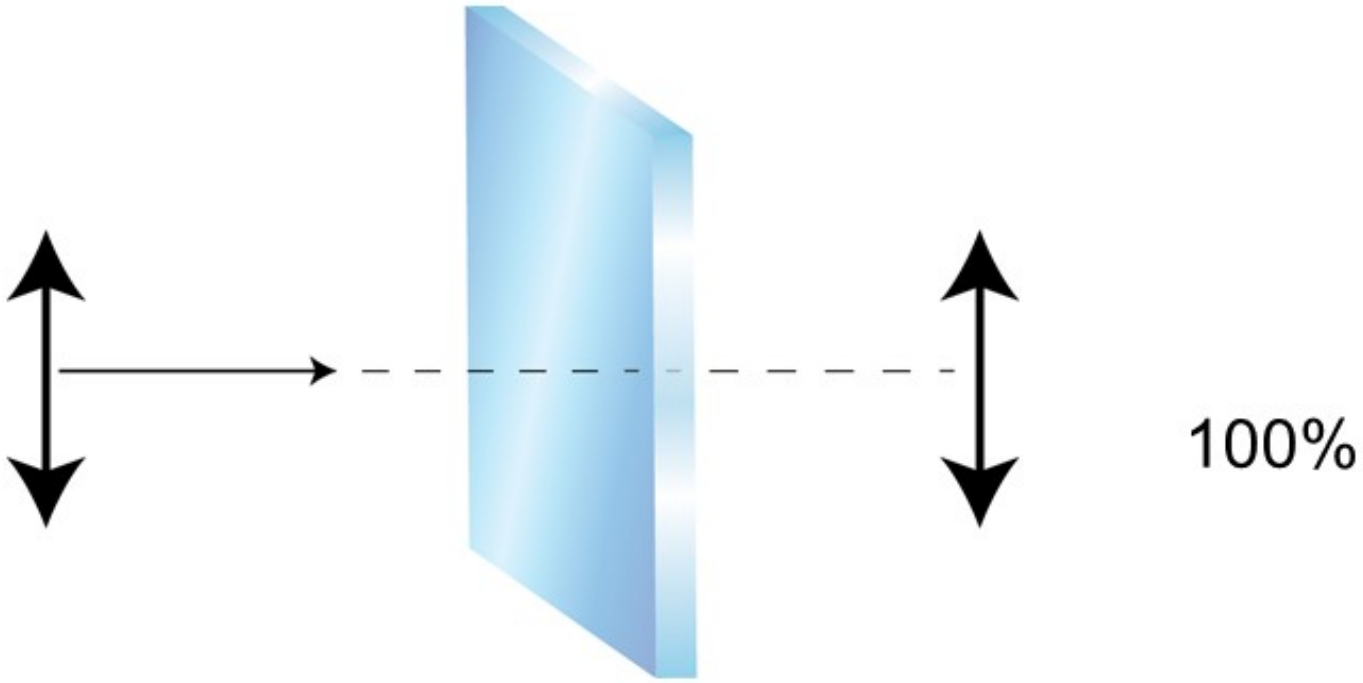
New feature: superposition/parallelism

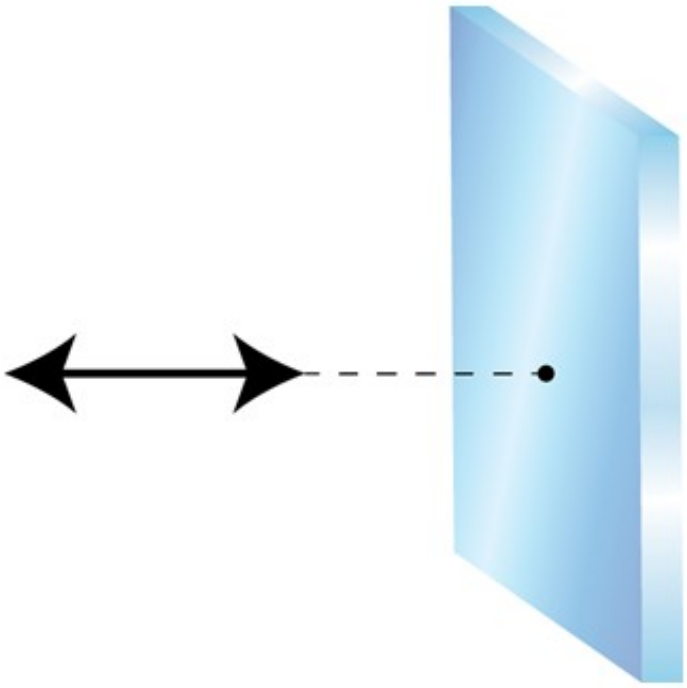
A physical system that can exist in two or more distinguishable states can in a special way embody all the distinguishable states at the same time



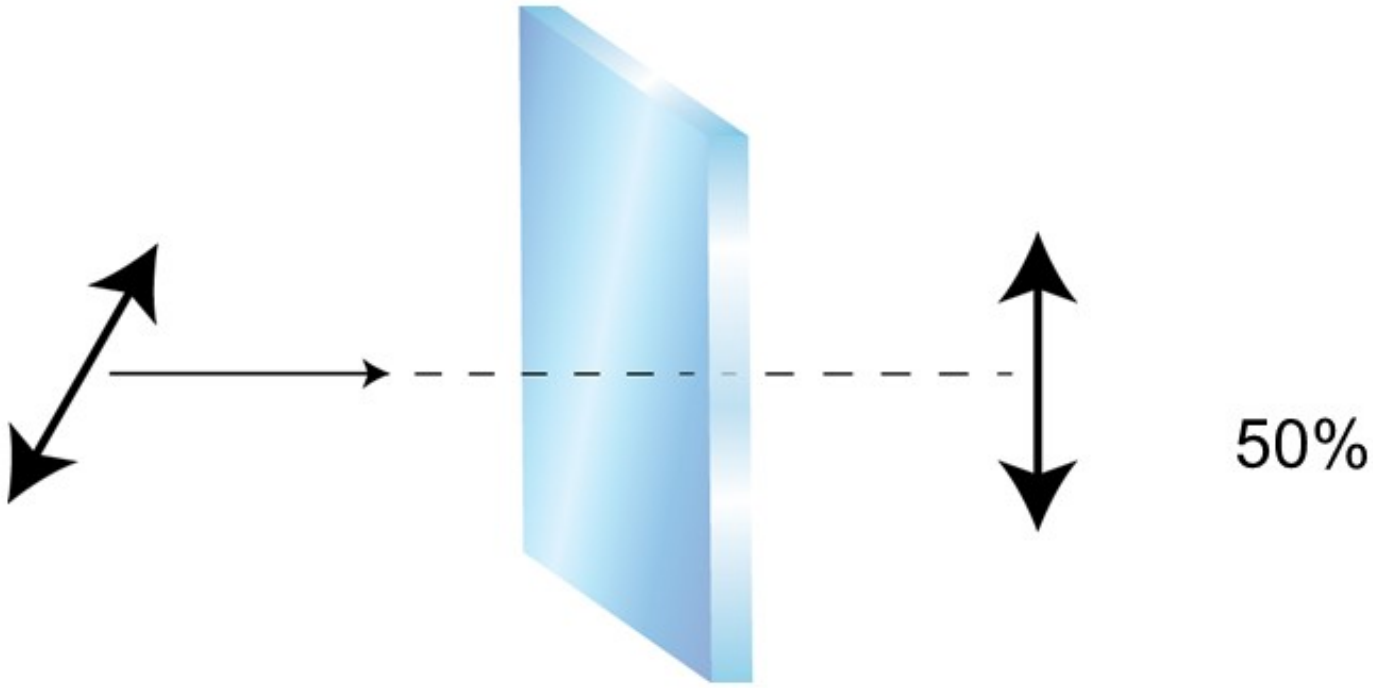

$(0.7071)^2$
$(-0.7071)^2$
0.7071
-0.7071

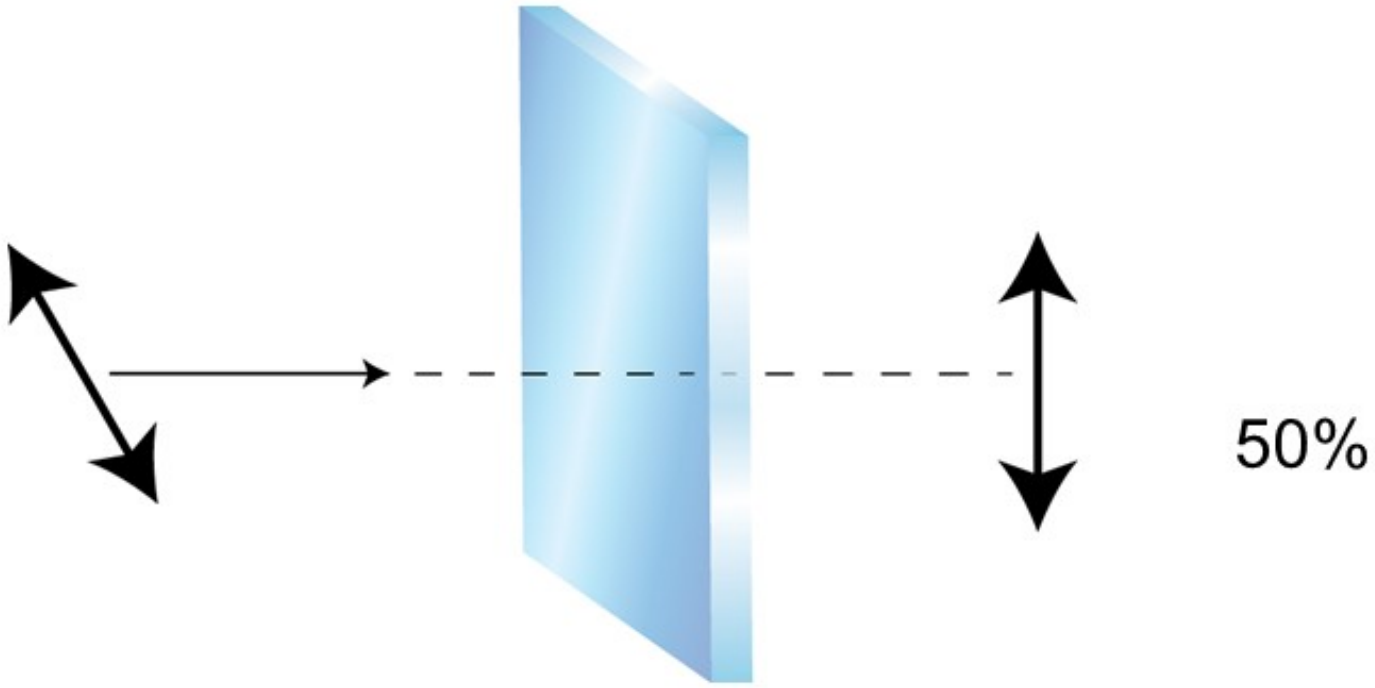
Superposition/parallelism

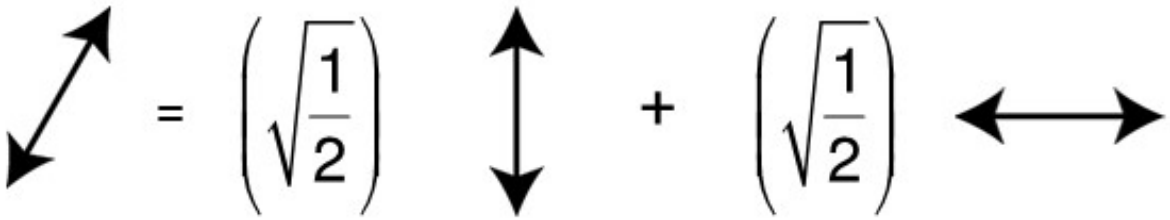


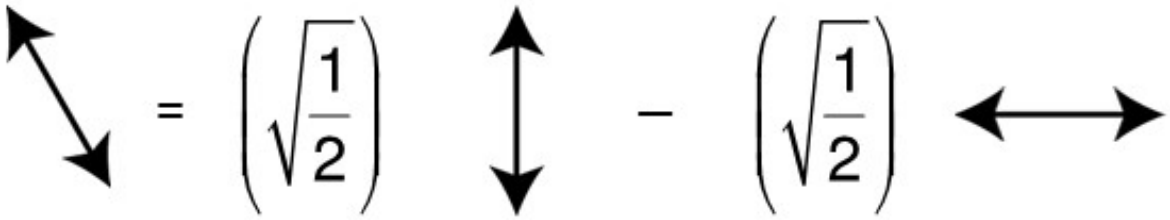


0%

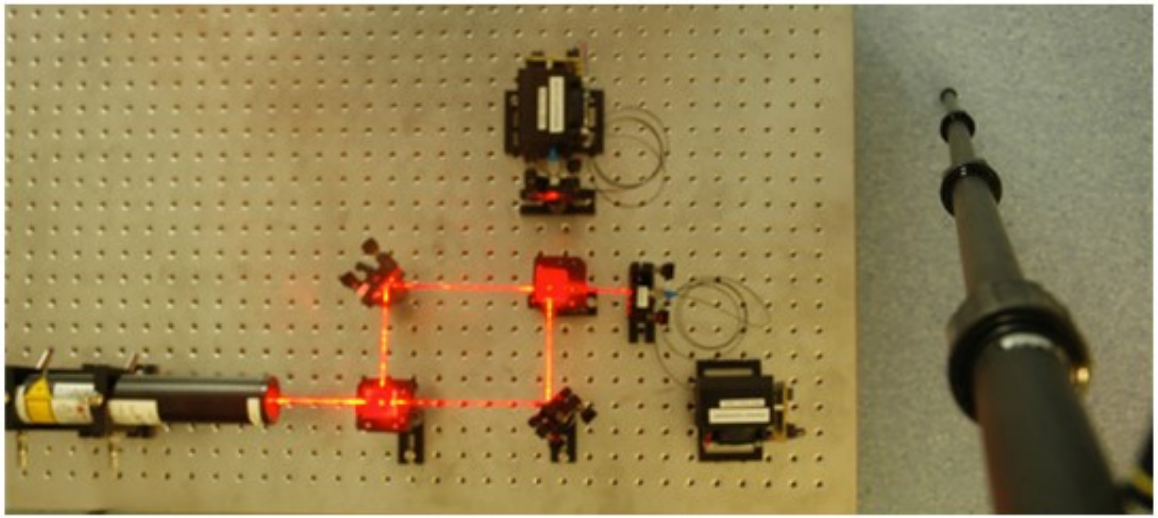

50%


50%

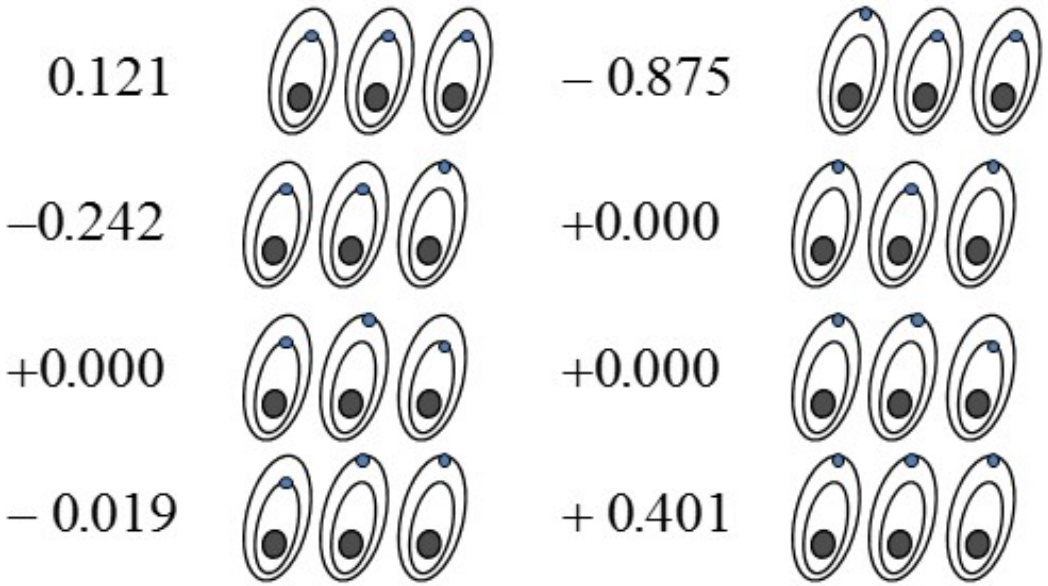




Superposition/parallelism



Dave Bacon's photo of Antia Lamas-Linares' lab at NUS Singapore


0.121
– 0.875
–0.242
+0.000
+0.000
+0.000
– 0.019
+ 0.401

What are quantum computers good for?

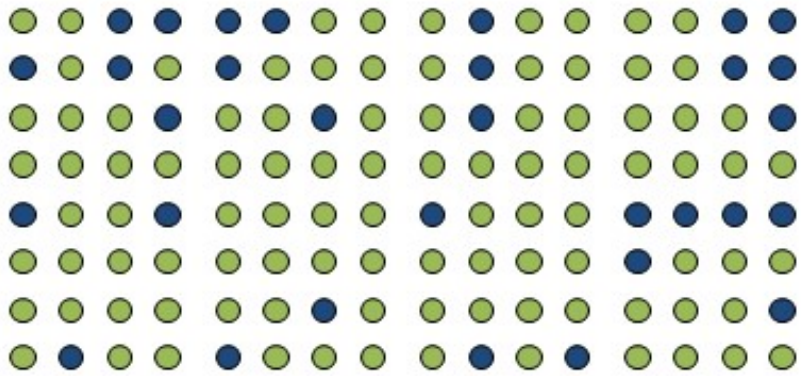
"Global" patterns: Seeing the forest without observing the trees.

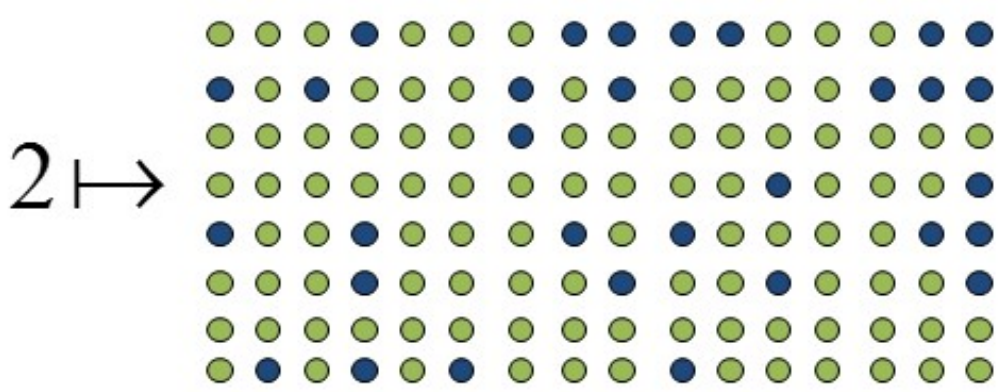
Example:

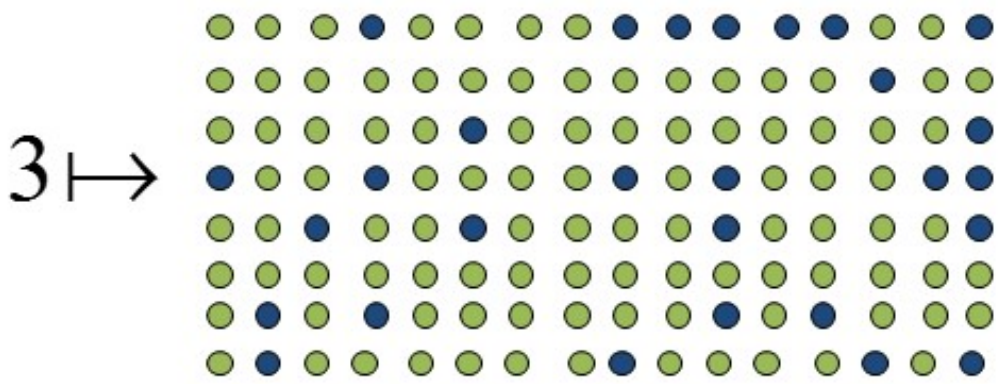
The sequence 34, 12, 54, 38, 57, 34, 12, 54, 38, 57, 34, 12, … has a *period* of length 5.

Example

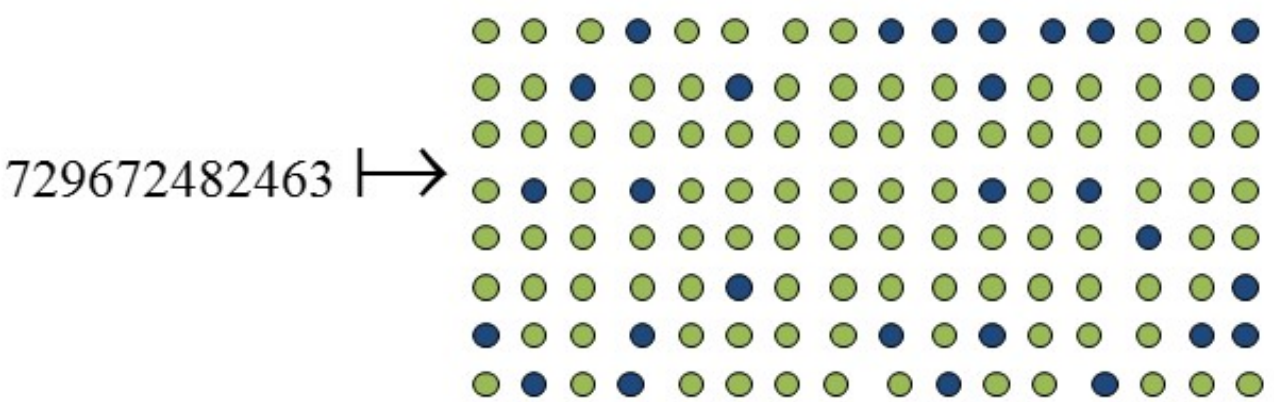
- Imagine a sequence of 128-bit numbers (encoded as bits) that can be easily computed

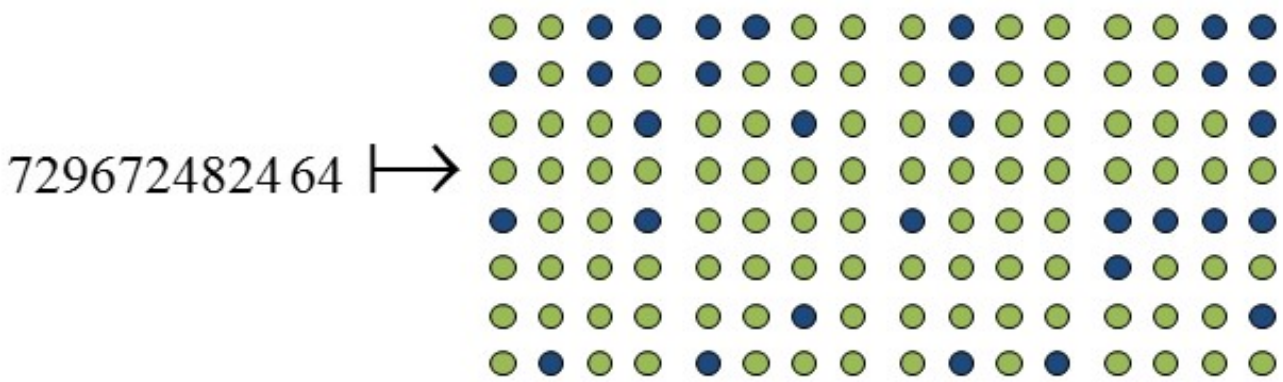
$1 \mapsto$ 


2 ↦

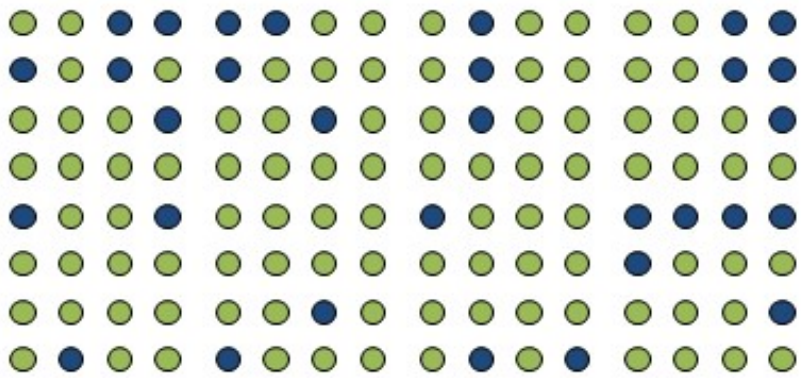

3 ↦

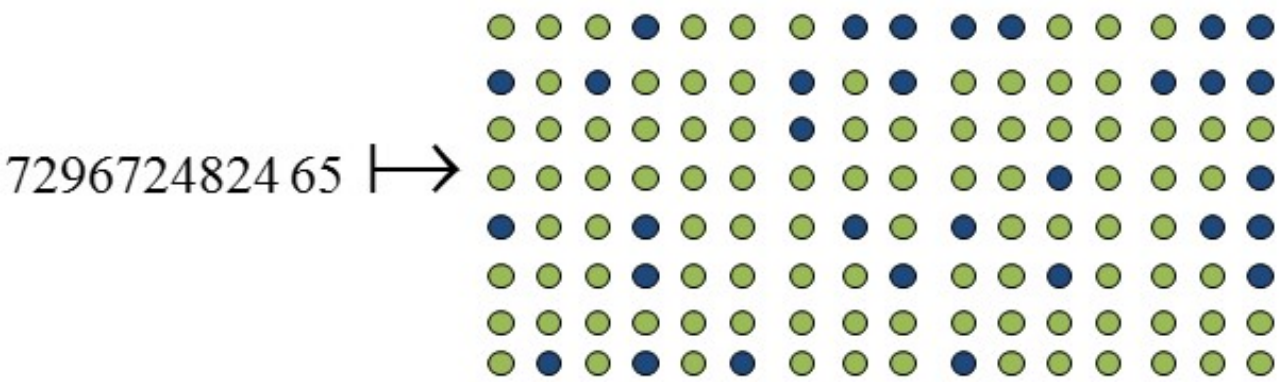
etc.


729672482463

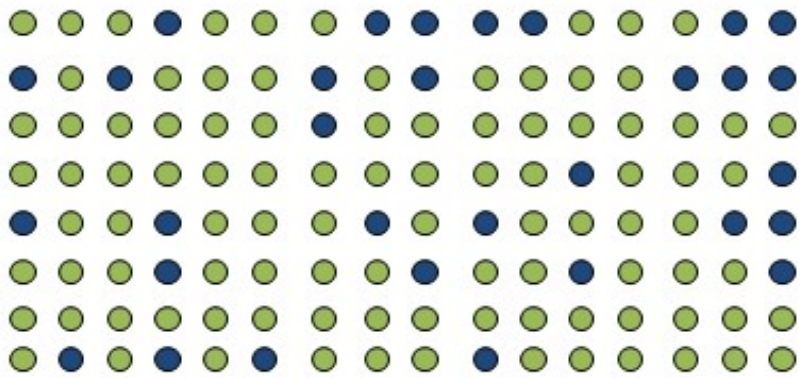

729672482464

(recall….)

$1 \mapsto$ 


72967248246 5

(recall…)

$2 \mapsto$ 

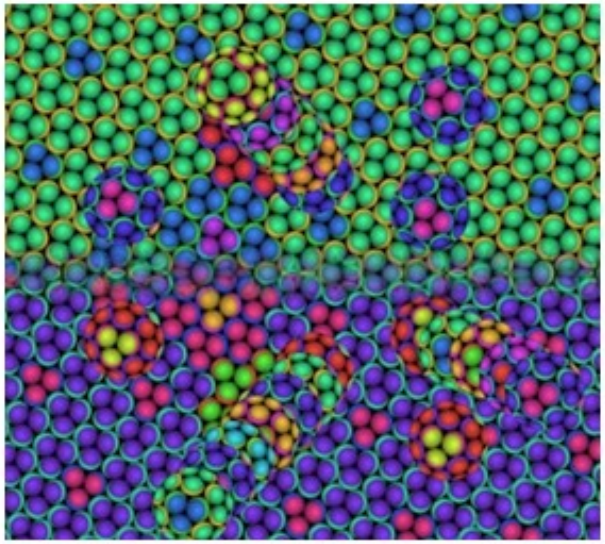
Example

With a handful of quantum glimpses:

"length of period = 729672482463"

"any specific value in the sequence = ???"

Applications:
studying materials and chemicals



Applications: Searching and Optimizing

Applications: Searching and Optimizing

"needle in a haystack"

$$\frac{1}{1000000}$$

$$\frac{1}{1000000}$$

$$\frac{1}{1000000}$$

$\ldots$

$$\frac{1}{1000000}$$




$$\frac{1}{1000000} \quad \frac{1}{1000000} \quad \frac{1}{1000000} \quad \cdots \quad \frac{1}{1000000}$$




$$\pm\frac{1}{1000} \quad \pm\frac{1}{1000} \quad \pm\frac{1}{1000} \quad \cdots \quad \pm\frac{1}{1000}$$




$$\pm\frac{1}{1000} \qquad \pm\frac{1}{1000} \qquad \pm\frac{1}{1000} \qquad \cdots \qquad \pm\frac{1}{1000}$$

Quantum computer finds a solution after roughly 1000 queries.

New feature:
Eavesdropper detection

Quantum Cryptography

Courtesy of Qiang Zhang, USTC

Beijing-Shanghai QKD Backbone

swissquantum.idquantique.com/?-Network-

SwissQuantum Network

http://www.uqcc.org/QKDnetwork/

Tokyo QKD Network

http://www.battelle.org/our-work/national-security/cyber-innovations/quantum-key-distribution

Battelle QKD Network Columbus, Ohio, USA

http://www.idquantique.com/photon-counting/clavis3-qkd-platform/

http://www.quantum-comm.com/index.php/Cate/index/pid/1

http://www.qasky.com/Product.aspx?id=94

Free-space Quantum Cryptography

Thomas Jennewein et al., Smiths Falls, Ontario, Canada, Sept. 2016

THE WALL STREET JOURNAL.

China Rethinks Its Alliance With Reeling Venezuela

Syria Rebels Press Fight Against Assad

Libyan Forces Loyal to Eastern Government Attack Key Oil Ports

New Tricks Make ISIS, Once Easily Tracked, a Sophisticated Opponent

WORLD | ASIA | CHINA NEWS

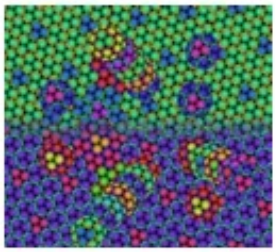
China's Latest Leap Forward Isn't Just Great—It's Quantum

Beijing launches the world's first quantum-communications satellite into orbit

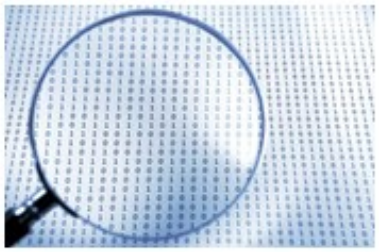
Long term future applications

Quantum money

New paradigm brings new possibilities



Designing new materials, drugs, etc.



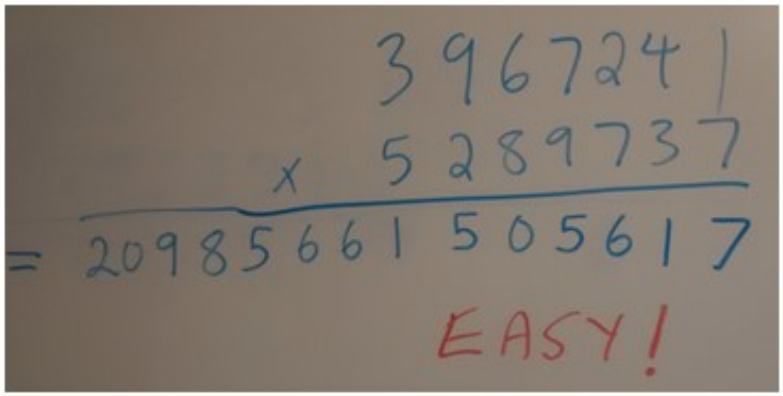
Optimizing

Sensing and measuring

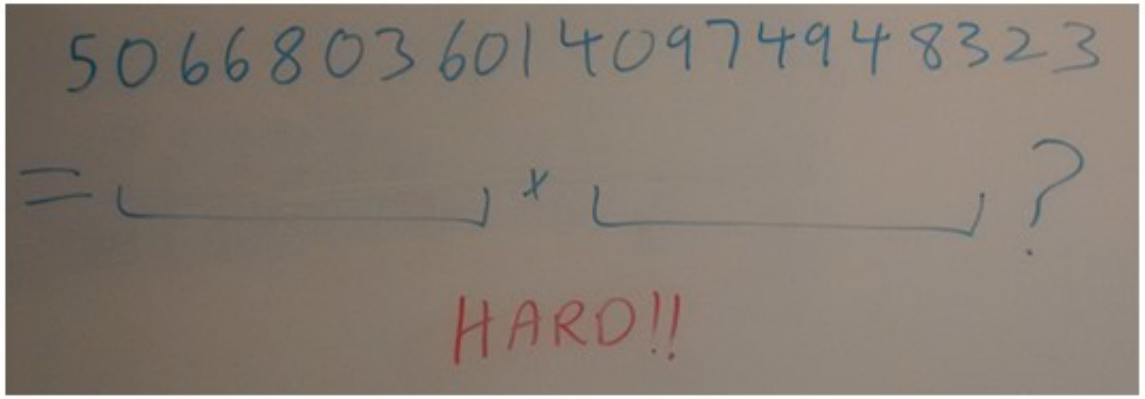
Secure communication

What else???

But… while in the old paradigm

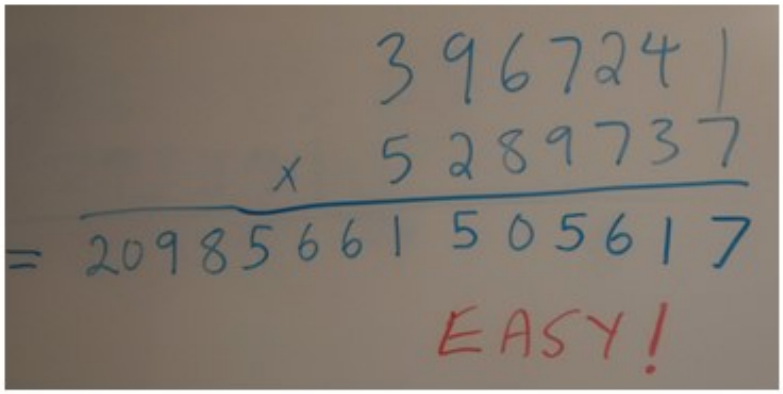


Encrypting is easy.

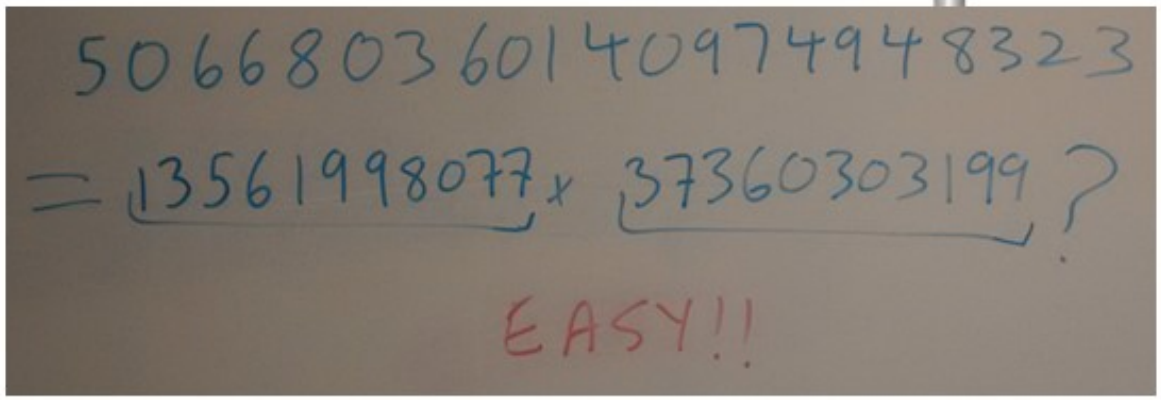


Codebreaking is hard.

…in the quantum paradigm

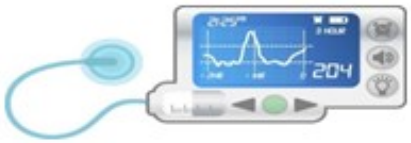


Encrypting is easy.



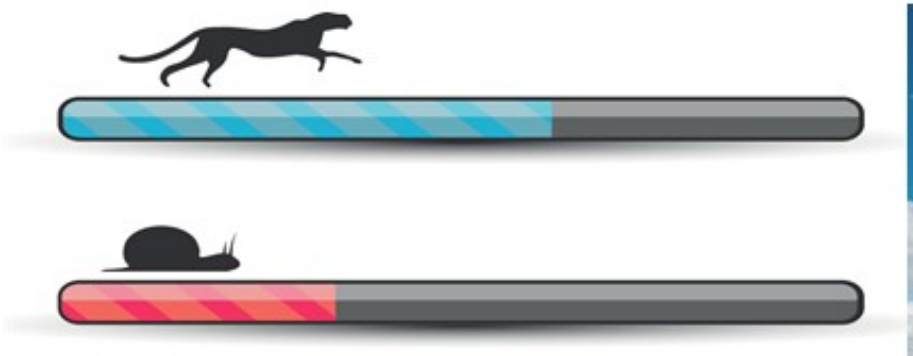
Codebreaking is **easy**!

Cyber technologies are everywhere



So cyberattacks are a growing threat

Price of procrastination?



Do we need to worry *now*?

Depends on:

- X = *security shelf-life*
- Y = *migration time*
- Z = *collapse time*

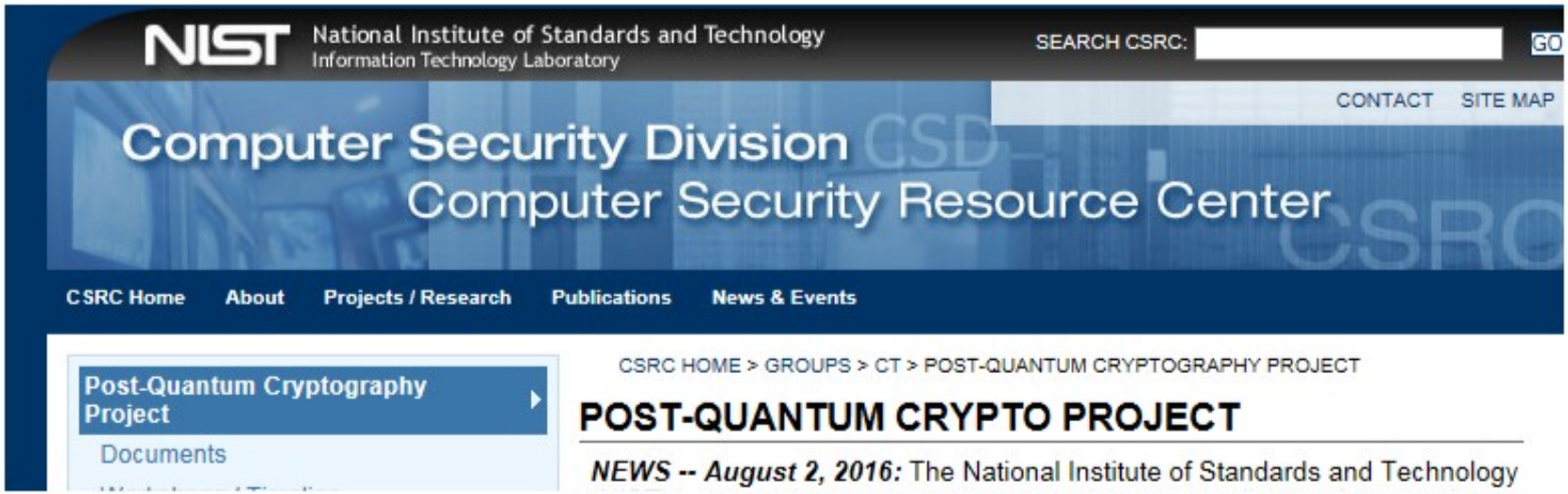
"Theorem": If $X + Y > Z$, then worry.

Bottom line

Fact: If X+Y>Z, then you will not be able to provide the required X years of security.

Fact: If Y>Z then cyber systems will collapse in Z years with no quick fix.

Security is a choice


NIST
National Institute of Standards and Technology
Information Technology Laboratory
SEARCH CSRC:
GO
CONTACT
SITE MAP
Computer Security Division
Computer Security Resource Center
CSD
CSRC
CSRC Home
About
Projects / Research
Publications
News & Events
Post-Quantum Cryptography Project
Documents
CSRC HOME > GROUPS > CT > POST-QUANTUM CRYPTOGRAPHY PROJECT
POST-QUANTUM CRYPTO PROJECT
NEWS -- August 2, 2016: The National Institute of Standards and Technology

4th ETSI-IQC Workshop on Quantum-Safe Cryptography

IT WORLD CANADA

CIO CSO MOBILE STORAGE CLOUD RESEARCH EVENTS NEWS VIDEO BLOGS MORE

Prepare for threat of quantum computing to encrypted data, Canadian conference told

Howard Solomon - September 20, 2016

"I think we are already behind," Scott Jones, deputy chief of IT security at the Communications Security Establishment (CSE), responsible for securing federal information systems, told the fourth annual international workshop on quantum-safe cryptography in Toronto on Monday.

NATIONAL POST

FINANCIAL POST • NEWS • COMMENT • PERSONAL FINANCE • INVESTING • TECH • SPORTS • ARTS • LIFE • HEALTH • HO

NEWS CANADA POLITICS

CANADIAN POLITICS

TRENDING Blue Jays | Brangelina | Trump | Clinton | Real estate | World Cup of Hockey | Lotto Max

Quantum computing will cripple encryption methods within decade, spy agency chief warns

IAN MACLEOD, OTTAWA CITIZEN | September 23, 2016 7:54 PM ET
More from Ian MacLeod, Ottawa Citizen

Republish
Reprint

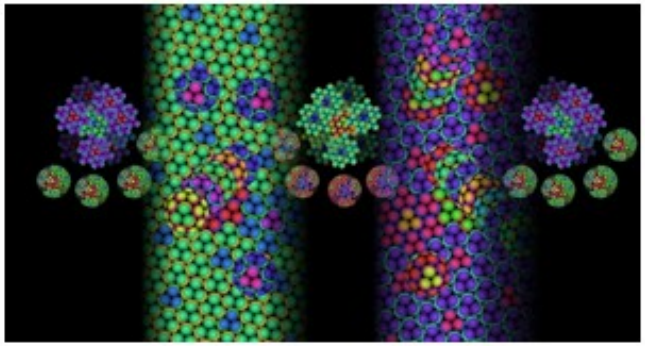
The choice is ours

Embrace quantum technologies that will help humanity
and
live in a (relatively) safe cyber-enhanced world?

☑ Yes

☐ No

Beyond next generation ICT



Quantum information science and technology: growing field

- Deep and broad roots
- Bearing fruit and bringing oxygen to a broader ecosystem

THANK YOU!!