Quantum Technology: Challenges and Opportunities for Cyber Security

Yaoyun Shi
University of Michigan
The Alien Monsters Are Coming!

Written by Yaoyun Shi
Illustrated by Oriana Shi
Surrender, Earthlings.

Your cyber space has no defense against our technology.

P.S.

- These are the secret keys you are using…
- We know all the secret keys that you are yet to use….
- And the roster of members for a super secretive website.
Isn’t our encryption secure?! 

Yes but only when on is not smart enough to break it...
Gur qnja bs pelcgbtencul
Gur qnja bs pelcgbtencul

credit: wikipedia
The diagram illustrates the ROT13 encryption scheme.

There are two rows of characters representing the alphabet:

1. Uppercase: A B C D E F G H I J K L M
2. Lowercase: n o p q r s t u v w x y z

Each character in the top row is shifted 13 places to the right in the bottom row. For example, A maps to N, B maps to O, and so on. This process is reversible, meaning the same characters are used to encrypt and decrypt messages.

Credit: Wikipedia
The dawn of cryptography

credit: wikipedia
The dawn of cryptography

- 2,500 years ago: substitution cypher
- Probably pretty secure
- Provable secure under the assumption that no one is smart enough to break it
Modern cryptography: a fortress built on sand

- The security of almost all crypto protocols are based on assumptions
- The hardware random number generator does generate secret keys
- The adversary is computationally limited
Modern cryptography: a fortress built on the sands

• Representative in public key cryptography:

  • RSA assumes hardness of factoring pq for large primes p and q

  • Elliptic Curve Cryptography (ECC) assumes hardness of computing discrete logarithm

• Obviously much more secure than ever

• But still assuming no one is smart enough to crack it
What exactly do they get?

Quantum computers
Quantum attack!

- Shor 1993: Fast quantum algorithms for factoring and discrete logarithms
- Any public key cryptography based on factoring and discrete logarithm will not be secure when a large quantum computer is built
Quantum computers

- Classical bits: 0 or 1, or a probabilistic mixture of them
- Quantum bit (qubit)
  - linear combination of 0 and 1
  - allows many different ways of observing a bit (0/1; +/-)
  - result to observation not pre-determined
- Multiple qubits can correlate in a fundamentally non-classical way
- Writing down how N quits would behave requires exponential in N bits of classical information

\[ \frac{(\text{love} - \text{hate})}{\sqrt{2}} \]

Will you marry me?

I didn't know but now you asked,
Quantum computers

- Multiple qubits can correlate in a fundamentally non-classical way
- Writing down how N quits would behave requires exponential in N bits of classical information
Quantum Speedup

- Deterministic algorithms: the next step is unique determined.

- Randomized algorithms: many next steps but once a mistake is made, no way to erase it.

- Quantum algorithms: many next steps, “mistaken” branches may cancel out by “interfering” with each other, leaving mostly the correct path.
Can’t we build a quantum computer?

Yes we can. .... but it takes time, and
When will there be a quantum computer?

- D-wave Systems: We make them, want to buy one?
- Being disputed, but for sure D-wave computers can’t factor
- They run a specific quantum heuristic not able to implement Shor’s algorithm
When will there be a quantum computer useful for cryptanalysis?

- We know no fundamental reason that it can’t be built
- Heavy investments from governments and companies
  - Europe: UK, Switzerland, …
  - Canada, China, Australia, Singapore,…
  - IBM, Microsoft, Google, …
Steady progress but breakthrough is yet to come

• Main challenge: how to scale up?

• Quantum mechanics governs microscopic world yet quantum computer needs to be massive

• Decoherence: protecting quantum bits from being corrupted
Steady progress but breakthrough is yet to come

• What makes the best physical quantum bit?

• Current candidates difficulty to scale up

• A possible silver bullet known theoretically but is yet to be experimentally realized
How do we defend ourselves?

Quantum-resilient classical cryptography and quantum cryptography
“Post-quantum” crypto

• Post-quantum: believed to be resilient to quantum attack

• Candidates: based on lattice/“learning with error” problems

• Becoming more and more practical

• Likely the direction of new standards and guidelines

Photo credit: wikipedia
NSA’s announcement on “Suite B”

“Currently, Suite B cryptographic algorithms are specified by the National Institute of Standards and Technology (NIST) and are used by NSA's Information Assurance Directorate in solutions approved for protecting classified and unclassified National Security Systems (NSS). Below, we announce preliminary plans for transitioning to quantum resistant algorithms.”

https://www.nsa.gov/ia/programs/suiteb_cryptography/

August 19, 2015
Response

- Know that the sky is not falling yet but will some day
  - Be informed of the new standards and guidelines
  - Be informed of the progress in quantum IT
- Know that what you consider ironclad encryption will have no protection then
- Apply extra protection on data that need to be secure for N years (say N=10)
  - Longer key length and extra layer of believed quantum-resilient protection
Quantum cryptography can provide unconditional security even against quantum attacks.
Quantum Key Distribution (QKD)

- Alice and Bob want to establish a secret key through a public conversation
- A basic primitive classically impossible to be unconditionally secure
- Unconditionally secure QKD are known and on the market

ID Quantique's QKD Server
Quantum Key Distribution (QKD)

- Non-cloning Theorem: no quantum xerox machine to clone an unknown quantum state
- If Eve gains substantial information, she will necessarily disturb the communication, which can be detected

Let's restart.
Quantum IT

• Multiple companies selling QKD products

• 1 quantum computing company and more to come

• Be an investor and an early adopter
  • This is the dawn of Quantum IT, be an industry leader and stakeholder
  • Extra assurance to the consumer, Asymmetry against competitors
How can I trust these quantum stuffs? I have no quantum sense.

You don’t have to....
Quantum Cryptograph 2.0: Trustworthy Quantum Information

- You can use a quantum device without trusting its integrity yet still reap the quantum benefit
- Prime examples: random number generation and key distribution
The Case of Randomness: between faith and reality
Randomness = Secrecy

Perfect secrecy/random

Almost perfect secrecy/random
Randomness is indispensable in reality

- Random Number Generators (RNGs) provide the mother secret for cryptography

- RNGs are in all computers/smart phones

- Hardware generator: Intel’s on-chip generator RdRand/ RdSeed

- Software generator: Linux’s /dev/random

- 100 T bits/day worldwide?
  - Each computer process uses randomness in starting: Address space layout randomization

- We trust that they are doing their jobs
Randomness is a faith: can’t test randomness directly

NINE NINE NINE NINE

ARE YOU SURE THAT’S RANDOM?

THAT’S THE PROBLEM WITH RANDOMNESS: YOU CAN NEVER BE SURE.
Randomness is a faith

NIST DRAFT Special Publication 800-90B

Recommendation for the Entropy Sources Used for Random Bit Generation

Elaine Barker
John Kelsey

Computer Security Division
Information Technology Laboratory

COMPUTER SECURITY

August 2012
Randomness is a faith

“[We assume] that the developer understands the behavior of the entropy source and has made a good faith effort to produce a consistent source of entropy.”
Current solutions are all trusted solutions: require blind faith
Blind faith is dangerous

- Lack of entropy causes weak cryptography keys [Heninger+, Lenstra+]
- Backdoors may be in government standards for RNGs [Snowden]
- Hardware may be maliciously modified
  - [Becker+’13]: Changing the dopant-level in Intel’s RNG can essentially remove the output randomness
The Aliens may have compromised all RNGs.

No more secret... even the weather forecast could be wrong.
A quantum solution to the trust problem

- Instead of testing randomness directly (which is impossible), test quantum-ness.
- Quantum-ness implies randomness.

[Colbeck’06]
The Mermin-Peres Magic Square Game

• A magic square: 3 by 3 table of 0/1
  • Each row sum is odd but each column sum is even
  • Impossible: summing up rows gets an even parity but summing up columns gets an odd parity

• The game: Alice/Bob are asked to output a randomly selected row/column satisfying the sum constraints. The intersection entry must be the same

• No classical strategy can win with more than 8/9 chance
  • Quantum can win all the time
Quantum entanglement: “Spooky action at a distance”

- Alice and Bob share “entanglement,” a bipartite quantum state
  - E.g., the Einstein-Podolski-Rosen state
- Alice’s action on her part “collapses” Bob’s part to a certain state
- The correlation between input/output cannot be produced by classical means

God doesn’t roll dice!
Being quantum is being random

- Any near optimal quantum strategy for the magic square game must produce universally random output.

- By checking the frequency of winning in a sequential run, we obtain proofs of the output randomness.
Untrusted-device randomness generation

- Need “seed” randomness to do test
- The seed can be super short, can be imperfect and can even be known to the adversary
- The output randomness can be made arbitrarily long

- Key features impossible classically
  - **Assurance**: the user knows that s/he is getting uniform randomness
  - **Trustworthiness**: the user needs not trust the integrity of the hardware (buying from the adversary is Okay)
Generating private randomness from public randomness

- NIST’s Randomness Beacon project: broadcasting public randomness
- Can be used to seed the Miller-Shi expansion protocol
Trustworthy Quantum Information in Michigan

• Working to implement prototypes for trustworthy quantum RNGs and key distribution systems
  • Funded by National Science Foundation (Co-PIs Carl Miller and Kim Winick)

• Investing other applications of trustworthy quantum information

Collaborator Prof. Kim Winick’s lab at U Michigan
Trustworthy Quantum Information in Michigan

The First International Workshop on Trustworthy Quantum Information took place in the past summer.

Co-organizers: Roger Colbeck (York), Xiongfeng Ma (Tsinghua), Stefano Pirandola (York)
Conclusions

• Cyber security’s very foundation is being threatened by quantum cryptanalysis

• Quantum crypto offers unprecedented level of protection to cyber security

• Quantum crypto can be made trustworthy

• Stronger classical crypto may be transitional or classical crypto vs quantum attack may persist

• Quantum IT is becoming real

• Watch out, get ready, and participate!
Acknowledgment

- Carl Miller and Jim Morgenstern
- Oriana Shi for inspiration of the aliens story and illustration
They are coming!

Photo Credit: earthsky.org