Mathematical Challenges in Security

What Quantum Computing means for cybersecurity

Richard Pinch

Researcher, Heilbronn Institute for Mathematical Research

7 September 2023

Outline

1. Computing
2. Cyber
3. Cryptography old and new
4. Post-modern cryptography
5. SOLILOQUY
6. Challenges

Disclaimer

This talk does not represent the position of His Majesty's Government, GCHQ, HIMR or IMA.

Images from GCHQ archives are Crown Copyright and reproduced courtesy of Director GCHQ.

Disclaimer

This talk does not represent the position of His Majesty's Government, GCHQ, HIMR or IMA.

Images from GCHQ archives are Crown Copyright and reproduced courtesy of Director GCHQ.

Outline

1. Computing
2. Cyber
3. Cryptography old and new
4. Post-modern cryptography
5. SOLILOQUY
6. Challenges

Computation

Alan Turing proposed the idea of the *Turing machine*: an abstract model of computation. The machine has a store ("tape") and at any given moment the machine is in a given "state". The transition from one state to the next is determined by the current state of the machine and the data currently stored.

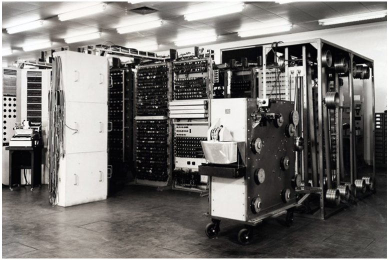
The *Church–Turing thesis* is that this model precisely captures all notions of computation and computability.

Computation

Alan Turing and Alonzo Church

Computation

Tommy Flowers and Colossus



Programming

> *The Analytical Engine has no pretensions whatever to originate anything. It can do whatever we know how to order it to perform.*

Ada Lovelace

Programming

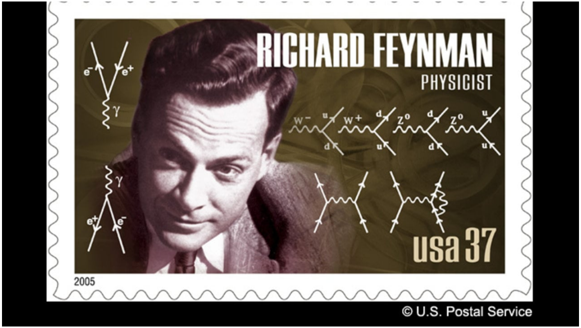
> *The Analytical Engine has no pretensions whatever to originate anything. It can do whatever we know how to order it to perform.*
>
> — Ada Lovelace

Programmes may however be randomised (use randomly generated data) and hence we may speak of results being “probabilistic”.

There are also real social and ethical concerns about results that we can neither understand nor verify.

Quantum computing

Richard Feynman was one of the first to suggest the application of quantum states to computation.



© U.S. Postal Service

In a modern (but still classical) digital computer, the store consists of discrete bits **0** and **1**, represented by physical states such as voltage (high/low). They are moved through circuits which perform Boolean operations such as

$$\mathrm{NOT} : \mathbf{0} \mapsto \mathbf{1}, \mathbf{1} \mapsto \mathbf{0};$$

$$\mathrm{AND} : \mathbf{00} \mapsto \mathbf{0}, \mathbf{01} \mapsto \mathbf{0}, \mathbf{10} \mapsto \mathbf{0}, \mathbf{11} \mapsto \mathbf{1}$$

and so on.

The mathematics of superposition

Some physical systems can be described by a simple set of states. For example, atoms in a crystal lattice having spin either up ↑ or down ↓.

If we consider three such atoms there are eight possible states

$$|\uparrow\uparrow\uparrow\rangle, |\uparrow\uparrow\downarrow\rangle, |\uparrow\downarrow\uparrow\rangle, |\uparrow\downarrow\downarrow\rangle, |\downarrow\uparrow\uparrow\rangle, |\downarrow\uparrow\downarrow\rangle, |\downarrow\downarrow\uparrow\rangle, |\downarrow\downarrow\downarrow\rangle$$

and we represent the superposition as a linear combination

$$\alpha_{000}|\uparrow\uparrow\uparrow\rangle + \alpha_{001}|\uparrow\uparrow\downarrow\rangle + \cdots + \alpha_{110}|\downarrow\downarrow\uparrow\rangle + \alpha_{111}|\downarrow\downarrow\downarrow\rangle$$

The coefficients α encode the probability ($|\alpha|^2$) of the system being found in that state when a measurement is made.

Entanglement

In this example the spins are *entangled* — that is, correlated.

For example

$$\frac{1}{\sqrt{2}}|\uparrow\uparrow\uparrow\rangle + \frac{1}{\sqrt{2}}|\downarrow\downarrow\downarrow\rangle$$

is an entangled state. If we measure it, and see that one atom is ↑ we immediately know that the others are also ↑.

This has been called “action at a distance”, and its precise nature is still a subject for philosophical debate. Nonetheless, entangled states exist in nature *and can be created in the laboratory*.

Quantum circuits

In a quantum computer, the store consists of entangled bits represented by physical states such as spin (up/down). They are moved through quantum circuits which respect the coherence of the states.

These circuits perform unitary operations which include some but not all Boolean operations, and some others.

$$\sqrt{\mathrm{NOT}} : |0\rangle \mapsto \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, |1\rangle \mapsto \frac{-1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle,$$

The reason for the notation is that applying $\sqrt{\mathrm{NOT}}$ twice yields the Boolean NOT operation.

Quantum computation

A quantum computer is composed of quantum registers (entangled bits) and quantum circuits that process these bits.

A computation consists of preparing the states (feeding in the data) and observing the result (reading out the answer). A quantum algorithm is a way of arranging the computation so that the desired answer emerges with high probability.

Comparison

Quantum computation is not a new paradigm in *computability* — it does not make it possible to compute anything that could not in principle also be computed on a Turing machine.

It is however a new paradigm in *complexity* — it makes it possible to solve certain kinds of problem in times significantly faster than classical computing.

Comparison

Quantum computation is not a new paradigm in *computability* — it does not make it possible to compute anything that could not in principle also be computed on a Turing machine.

It is however a new paradigm in *complexity* — it makes it possible to solve certain kinds of problem in times significantly faster than classical computing.

Complexity

There is a rich theory of complexity classes of problems with respect to classical computation, and the requirements of both time and space to solve them.

Problems are typically characterised by the number of bits (digits, symbols) required to describe them.

We may distinguish two major classes: *exponential* time and *polynomial* time.

Complexity classes

Exponential time algorithms typically include some form of "brute force" search. For example, to find a solution to an equation $f(x) = y$ with no further knowledge of the structure of the possible solution set would require the exhaustive test of all possible x until the correct answer is found.

Polynomial time algorithms typically involve knowledge of structure, such as linear programming, in which the linear nature of the problem and the constraints allow the solution to be "approached" or approximated.

Quantum algorithms

Three essentially quantum algorithms have been discovered.

- *Grover's algorithm*. Speeds up any brute force search. A space of size 2^n can be searched exhaustively in only $2^{n/2}$ steps.
- *Shor's algorithm*. A number theoretic algorithm which solves factorisation of large numbers in polynomial time.
- *SOLILOQUY*. Another number theoretic algorithm for finding hidden structure in combinatorial problems. Discovered by GCHQ/HIMR researchers around 2007-8 and published in 2014. Thought to be polynomial time.

National Quantum Computing Centre

Image courtesy NQCC and Hawkins/Brown

Practicalities

Quantum algorithms assume the existence of *logical* qbits: quantum bits exhibiting perfect quantum behaviour. Practical implementations require multiple physical qbits to represent a logical qbit in a reliable way. Maintaining qbits in a quantum state and moving information through a quantum circuit requires new form of error-correcting codes, such as *surface codes*, which model the nature of errors in quantum circuits.

Outline

1 Computing

2 Cyber

3 Cryptography old and new

4 Post-modern cryptography

5 SOLILOQUY

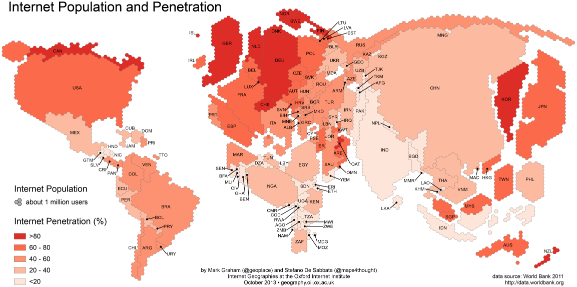
6 Challenges

Cyberspace

> *Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts.*
>
> — William Gibson (1984) *Neuromancer*

The internet world

Internet Population and Penetration



Internet Population

about 1 million users

Internet Penetration (%)

- ■ >80
- ■ 60 - 80
- ■ 40 - 60
- ■ 20 - 40
- ■ <20

by Mark Graham (@geoplace) and Stefano De Sabbata (@maps4thought)
Internet Geographies at the Oxford Internet Institute
October 2013 • geography.oii.ox.ac.uk

data source: World Bank 2011
http://data.worldbank.org

Cyberspace

> *The National Security Strategy categorised cyber attacks as a Tier One threat to our national security, alongside international terrorism. The threat to our national security from cyber attacks is real and growing. Terrorists, rogue states and cyber criminals are among those targeting computer systems in the UK.*
>
> — `https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace`

Outline

1. Computing
2. Cyber
3. Cryptography old and new
4. Post-modern cryptography
5. SOLILOQUY
6. Challenges

A brief history of cryptography

- Traditional cryptography — Secret key Julius Caesar 55BC (+3 mod 24) via one-time pad to the present day (AES, TLS/SSL, 3G, 4G)
- Modern cryptography — Public key Cliff Cocks 1972 (RSA) to the present day (RSA, DH, TLS/SSL)
- Post-modern cryptography — Quantum and post-quantum ~~2014~~ 2006 on

A brief history of cryptography

- Traditional cryptography — Secret key Julius Caesar 55BC (+3 mod 24) via one-time pad to the present day (AES, TLS/SSL, 3G, 4G)
- Modern cryptography — Public key Cliff Cocks 1972 (RSA) to the present day (RSA, DH, TLS/SSL)
- Post-modern cryptography — Quantum and post-quantum ~~2014~~ 2006 on

A brief history of cryptography

- Traditional cryptography — Secret key Julius Caesar 55BC ($+3 \bmod 24$) via one-time pad to the present day (AES, TLS/SSL, 3G, 4G)
- Modern cryptography — Public key Cliff Cocks 1972 (RSA) to the present day (RSA, DH, TLS/SSL)
- Post-modern cryptography — Quantum and post-quantum ~~2014~~ 2006 on

A brief history of cryptography

- Traditional cryptography — Secret key Julius Caesar 55BC (+3 mod 24) via one-time pad to the present day (AES, TLS/SSL, 3G, 4G)
- Modern cryptography — Public key Cliff Cocks 1972 (RSA) to the present day (RSA, DH, TLS/SSL)
- Post-modern cryptography — Quantum and post-quantum ~~2014~~ 2006 on

A brief history of cryptography

- Traditional cryptography — Secret key Julius Caesar 55BC (+3 mod 24) via one-time pad to the present day (AES, TLS/SSL, 3G, 4G)
- Modern cryptography — Public key Cliff Cocks 1972 (RSA) to the present day (RSA, DH, TLS/SSL)
- Post-modern cryptography — Quantum and post-quantum ~~2014~~ 2006 on

A brief history of cryptography

- Traditional cryptography — Secret key Julius Caesar 55BC $(+3 \bmod 24)$ via one-time pad to the present day (AES, TLS/SSL, 3G, 4G)
- Modern cryptography — Public key Cliff Cocks 1972 (RSA) to the present day (RSA, DH, TLS/SSL)
- Post-modern cryptography — Quantum and post-quantum ~~2014~~ 2006 on

A brief history of cryptography

- Traditional cryptography — Secret key Julius Caesar 55BC ($+3 \bmod 24$) via one-time pad to the present day (AES, TLS/SSL, 3G, 4G)
- Modern cryptography — Public key Cliff Cocks 1972 (RSA) to the present day (RSA, DH, TLS/SSL)
- Post-modern cryptography — Quantum and post-quantum ~~2014~~ 2006 on

A brief history of cryptography

- Traditional cryptography — Secret key Julius Caesar 55BC $(+3 \bmod 24)$ via one-time pad to the present day (AES, TLS/SSL, 3G, 4G)
- Modern cryptography — Public key Cliff Cocks 1972 (RSA) to the present day (RSA, DH, TLS/SSL)
- Post-modern cryptography — Quantum and post-quantum ~~2014~~ 2006 on

A brief history of cryptography

- Traditional cryptography — Secret key Julius Caesar 55BC (+3 mod 24) via one-time pad to the present day (AES, TLS/SSL, 3G, 4G)
- Modern cryptography — Public key Cliff Cocks 1972 (RSA) to the present day (RSA, DH, TLS/SSL)
- Post-modern cryptography — Quantum and post-quantum ~~2014~~ 2006 on

A brief history of cryptography

- Traditional cryptography — Secret key Julius Caesar 55BC ($+3 \bmod 24$) via one-time pad to the present day (AES, TLS/SSL, 3G, 4G)
- Modern cryptography — Public key Cliff Cocks 1972 (RSA) to the present day (RSA, DH, TLS/SSL)
- Post-modern cryptography — Quantum and post-quantum ~~2014~~ 2006 on

Cocks/RSA

The user’s secret is the factorisation of a large number N.

The user’s identifier has been bound to N by some chain of trust.

To authenticate the user performs a mathematical operation which only someone who knows the factors of N could do (in any reasonable amount of time).

Outline

1 Computing

2 Cyber

3 Cryptography old and new

4 **Post-modern cryptography**

5 SOLILOQUY

6 Challenges

Post-modern cryptography

Future directions in cryptography

Active areas of research include:

- Privacy-preserving computation
- Post-quantum cryptography

Post-modern cryptography

Future directions in cryptography

Active areas of research include:

- Privacy-preserving computation
- Post-quantum cryptography

Post-quantum cryptography

Classical cryptography for the age of the quantum computer.

Grover’s algorithm would solve exhaustion problems in square-root time.

Shor’s algorithm would solve factoring and discrete logarithm problems in polynomial time.

Post-quantum cryptography

Response to Grover's algorithm: double key sizes.

Response to Shor's algorithm: *new public-key systems needed*.
Some suggestions:

- hidden structure within error-correcting codes
- hidden structure within integer lattices (SOLILOQUY)
- low-weight solutions to garbled linear equations

Do we need public-key cryptography at all?

Post-quantum cryptography

Response to Grover's algorithm: double key sizes.

Response to Shor's algorithm: *new public-key systems needed*. Some suggestions:

- hidden structure within error-correcting codes
- hidden structure within integer lattices (SOLILOQUY)
- low-weight solutions to garbled linear equations

Do we need public-key cryptography at all?

Post-quantum cryptography

Response to Grover's algorithm: double key sizes.

Response to Shor's algorithm: *new public-key systems needed*. Some suggestions:

- hidden structure within error-correcting codes
- hidden structure within integer lattices (SOLILOQUY)
- low-weight solutions to garbled linear equations

Do we need public-key cryptography at all?

Error-correction

The leading methods proposed for new PK systems are based on error correction. The message is deliberately garbled and the recipient can correct the errors efficiently using private knowledge of some hidden structure.

There is a rich history of error-correcting codes with efficient error correction, based on algebraic structure, usually over the field $\mathrm{GF}(2)$ of two elements

There is a continuous analogue, based on finding the nearest element of a lattice (discrete subgroup of Euclidean space) to a given point

The NIST challenge

In 2016 NIST published a challenge for proposals for a new qunatum-resistent public key cryptosystem. There were over 70 entries, and most were based on some form of error-correction.

There is no clear “winner” yet . . .

The NIST challenge

In 2016 NIST published a challenge for proposals for a new qunatum-resistent public key cryptosystem. There were over 70 entries, and most were based on some form of error-correction.

There is no clear “winner” yet . . .

The McEliece proposal

Take an error-correcting code C with encoding e and decoding d. Let m be the desired message. Take a random word r and transmit $z = e(r) + m$. The recipient forms $e(z) = r$ and then finds $m = z - e(r)$. Note that r is a dummy: the message is m.

For this to be a PKC, the decoding must depend on some hidden structure known only to the recipient. The attacker is faced with a search for the “nearest” (in the sense of Hamming metric) codeword $e(r)$, which is in general hard.

Hidden structure

Fast decoding is highly desirable in practical error-correction schemes and many such schemes are known based on algebraic structures.

The challenge is to “scramble” the code parameters in such a way that the structure is hard to recover from the public data.

Outline

1 Computing

2 Cyber

3 Cryptography old and new

4 Post-modern cryptography

5 SOLILOQUY

6 Challenges

SOLILOQUY

SOLILOQUY is a lattice-based primitive designed by Dan Shepherd of CESG in 2007.

The public key for SOLILOQUY is very compact for a lattice-based PKC system, being only about the same size as a single RSA modulus.

GCHQ believes that SOLILOQUY is classically secure but was surprised to discover a quantum attack.

SOLILOQUY

The security of SOLILOQUY is based on the difficulty of two well-known hard problems.

Close **V**ector **P**roblem: Classical CVP difficulty via Lattice Basis Reduction is well understood. There is no known quantum speedup.

Principal **I**deal **P**roblem: Given a representation of a principal ideal $\mathcal{I}$ of $\mathcal{O}$, recover a small generator of the ideal. The known (at the time) classical and quantum algorithms are only practical for number fields of small fixed degree.

GCHQ/HIMR believed for some years that since SOLILOQUY used large-degree fields it should be quantum resistant.

Outline

1. Computing
2. Cyber
3. Cryptography old and new
4. Post-modern cryptography
5. SOLILOQUY
6. Challenges

Mathematical challenges 1: quantum algorithmics

- Understand quantum complexity relative to classical complexity
- Costing techniques for quantum algorithms
- Develop new quantum algorithms

Mathematical challenges 2: error-correction

- New classical algorithms for error-correction
- Classical algorithms for finding hidden structure
- Quantum algorithms for error-correction
- Quantum algorithms for finding hidden structure

Conclusion

Designing quantum-resistant cryptography is hard. It took GCHQ several years to develop SOLILOQUY and several more to investigate its potential quantum resistance.

At this time, when many novel types of quantum-resistant cryptography are being proposed, it is important that these receive a thorough independent asessment.

The state of play

Quantum computing is not the end of cryptography or of cyber-security — indeed it is just a new stage in its evolution. Academic, government and industrial researchers are working on post-quantum proposals and standards bodies are already developing proposals for new standards.

Mathematics will continue to be at the heart of cryptography in the post-modern era as it has been for the past 85 years.

The state of play

Quantum computing is not the end of cryptography or of cyber-security — indeed it is just a new stage in its evolution. Academic, government and industrial researchers are working on post-quantum proposals and standards bodies are already developing proposals for new standards.

Mathematics will continue to be at the heart of cryptography in the post-modern era as it has been for the past 85 years.

Questions Comments!

Questions?

Comments!