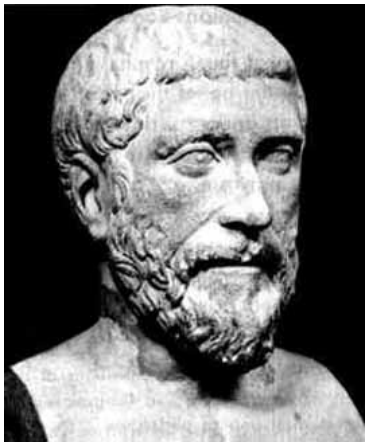
Pythagoras to Turing to Snowden
Diophantine equations, computation and privacy

Steven Galbraith

Mathematics Department, University of Auckland

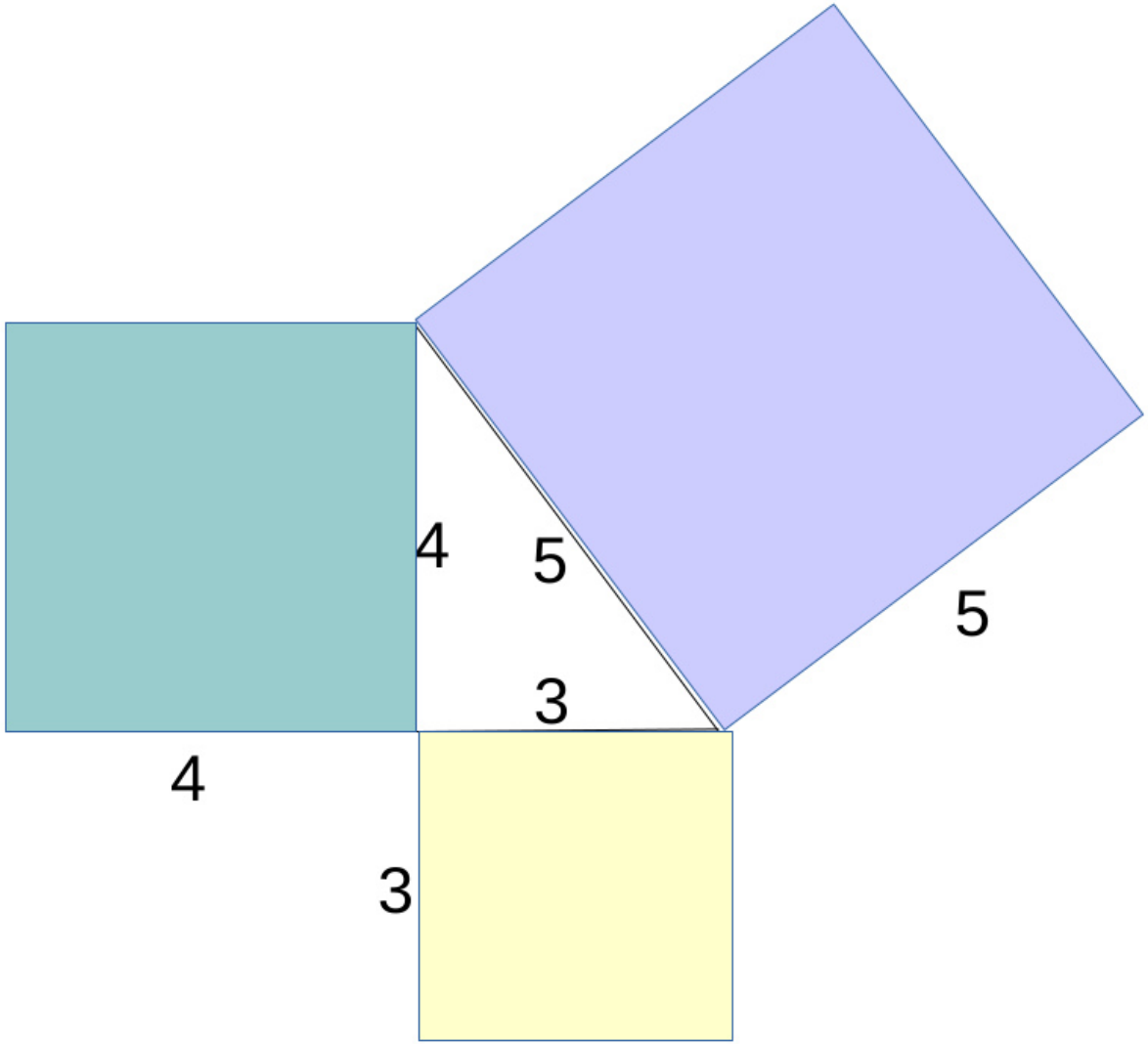


This is a revised and reduced version of the slides.
These slides are much less entertaining than the actual talk.
There is no substitute for the experience of being in the room.

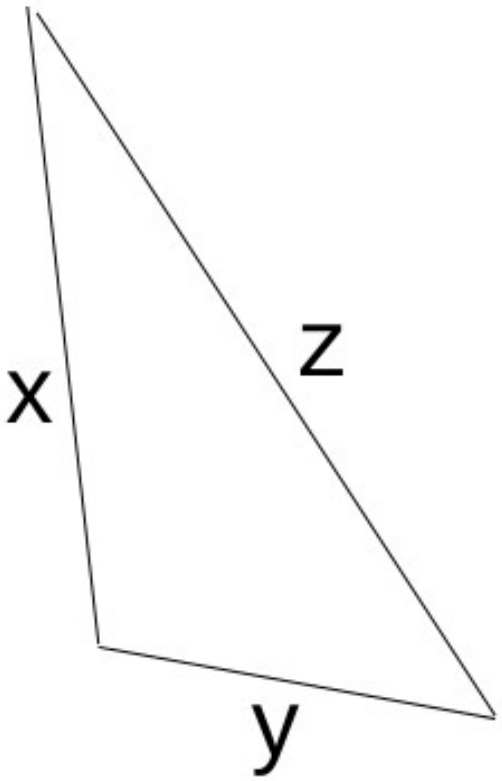
Welcome

Ko Rangitoto te maunga
Ko Kerikeri te awa
Ko Pupuke te moana
Ko Ngati Pakeha ahau
Ko Steven Galbraith tōku ingoa
Tēnā koutou, tēnā koutou, tēnā koutou katoa.

$9 + 16 = 25$



"Pythagoras Theorem"



- Triangle is right angle if and only if
$$x^2 + y^2 = z^2.$$
- This fact was known to Mesopotamian, Indian and Chinese mathematics before Pythagoras.
- For example, Babylonian mathematicians knew $799^2 + 960^2 = 1249^2$.

How many whole number solutions?

- We know that $(x, y, z) = (3, 4, 5)$ satisfies the equation

$$x^2 + y^2 = z^2.$$

- A pure mathematician asks:
  - Are there finitely or infinitely many integer solutions?
  - Is there a procedure to compute the integer solutions?
- Pythagoras is credited with the discovery that $(n^2 - 1, 2n, n^2 + 1)$ is an infinite set of solutions, where n is any integer.
- Euclid was the first to show that every solution is

$$(x, y, z) = (m^2 - n^2, 2mn, m^2 + n^2)$$

for some integers m, n.

Diophantus of Alexandria

- Lived maybe around 200AD.
- The "father of algebra" for his book Arithmetica.
- He studied the general problem of finding integer or rational solutions to systems of polynomial equations.

Projective to affine

Suppose $x^2 + y^2 = z^2$.

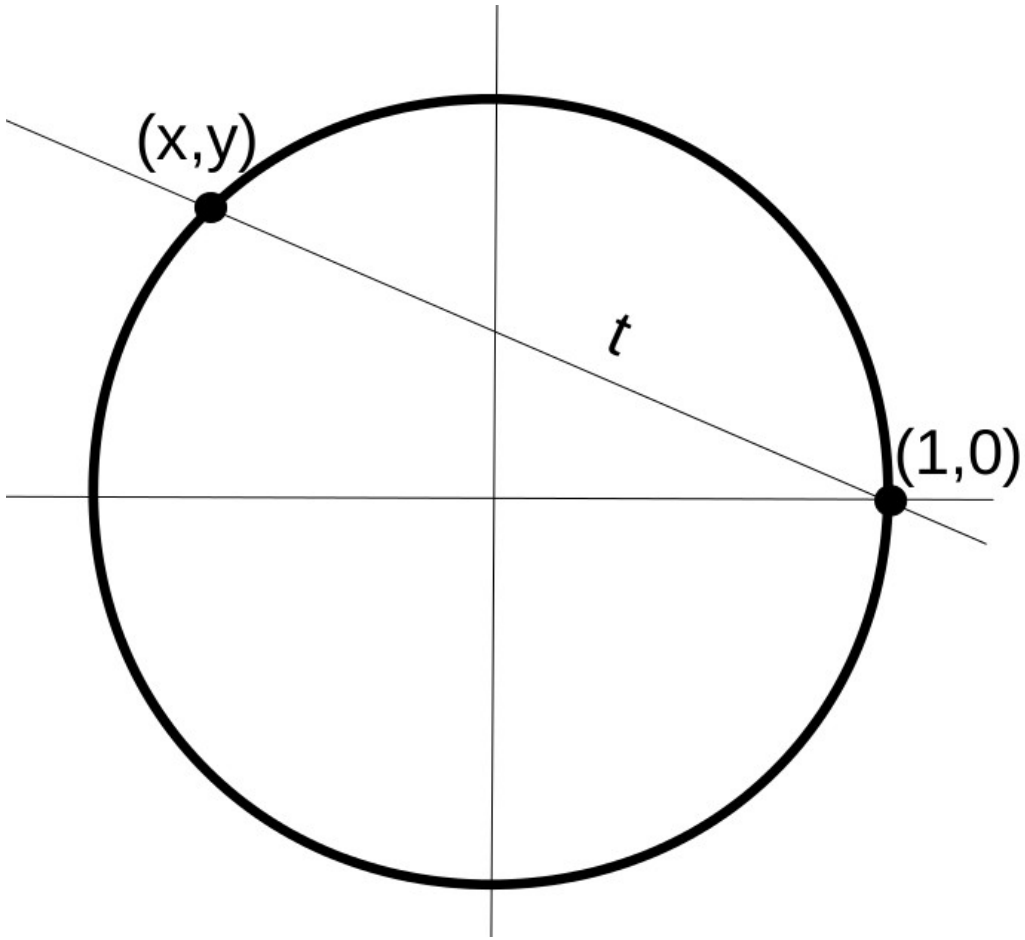
Dividing by z^2 turns an integer solution into a rational solution

$$\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1.$$

So now the integer solutions to the original equation become rational number solutions to a new equation $X^2 + Y^2 = 1$.

For example, the solution $(x, y, z) = (3, 4, 5)$ becomes $(X, Y) = (3/5, 4/5)$.

Points on the circle



$$(x, y) = ((t^2 - 1)/(t^2 + 1), -2t/(t^2 + 1))$$

Diophantine equations

A Diophantine equation is a system of polynomial equations with integer or rational number coefficients.

We are interested in solutions that are integers or rational numbers.

Example $X_0^+(311)$

$$x^2 + wy - 2xy + 2y^2 + 7xz - 8yz + 13z^2 = 0$$

$$wx^2 - 2wxy + x^2y - wy^2 - xy^2 - 2y^3 + w^2z + 6wxz$$
$$-x^2z - wyz + 5xyz + 4y^2z + 7wz^2 - 4xz^2 - 2z^3 = 0$$

Find integers w, x, y, z (not all zero) that satisfy both equations.

Diophantine equations

- The Indian mathematician Brahmagupta (598-670) studied Diophantine equations and computed the smallest non-trivial integer solution of $x^2 - 61y^2 = 1$ to be

$$(x, y) = (1766319049, 226153980).$$

- Persian mathematician Abu-Mahmud Khojandi (Al-Khujandi) (around 940-1000) tried to prove the equation

$$x^3 + y^3 = z^3$$

has no non-trivial integer solutions.

- Pierre de Fermat (1607-1665) wrote in the margin of his copy of Diophantus that if $n > 2$ then there are no non-trivial integer solutions to

$$x^n + y^n = z^n.$$

Fermat proved this result for $n = 4$.

Fermat's last theorem

"My butter, garçon, is writ large in!"
A diner was heard to be chargin'.
"I had to write there,"
exclaimed waiter Pierre,
"I couldn't find room in the margarine."

– Everett Howe, Hendrik Lenstra, David Moulton

The Purity of Mathematics: G. H. Hardy (1877–1947)

- *A mathematician, like a painter or a poet, is a maker of patterns. If his(sic) patterns are more permanent than theirs, it is because they are made with ideas.*
  – "A Mathematician's Apology".

- *A science is said to be useful if its development tends to accentuate the existing inequalities in the distribution of wealth, or more directly promotes the destruction of human life.*

- *No discovery of mine has made, or is likely to make, directly or indirectly, for good or ill, the least difference to the amenity of the world.*

The Purity of Mathematics

- It is comforting to work on problems that are motivated only by beauty, the culture of the subject, and one's own sense of pleasure.
- We expect the taxpayer to fund this, because the mathematics is ultimately useful and important.
- We encourage people to study mathematics, because it is useful.
- But we absolve ourselves of any moral responsibility for the mathematics we create/discover.

Hilbert (1862–1943)

- Incredibly wide-ranging and influential mathematician.
- G. H. Hardy ranked mathematicians on a scale of 0 to 100:

Hardy:	25
Littlewood:	30
Hilbert:	80
Ramanujan:	100

Hilbert's 1900 Lecture

- Hilbert gave a famous lecture at the International Congress of Mathematicians in Paris in 1900.
- His lecture comprised a list of 23 unsolved problems.

Who among us would not be happy to lift the veil behind which is hidden the future; to gaze at the coming developments of our science and at the secrets of its development in the centuries to come? What will be the ends toward which the spirit of future generations of mathematicians will tend? What methods, what new facts will the new century reveal in the vast and rich field of mathematical thought?

Hilbert's 10th problem

- The "Entscheidung" or "decision" problem.

  Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined in a finite number of operations whether the equation is solvable in rational integers.

- Is there an algorithm to determine if a Diophantine equation has a solution?

Alan Turing

- Worked on Hilbert's 10th. (Actually a "logic" version of Hilbert's 10th.)
- Major paper written as an undergrad at Cambridge in 1936 showed fundamental limitations on computing.
- Alonso Church had similar result about the same time.
- Turing did his PhD in Princeton supervised by Church, and returned to England in 1938.

ON COMPUTABLE NUMBERS, WITH AN APPLICATION TO THE ENTSCHEIDUNGSPROBLEM

By A. M. TURING.

[Received 28 May, 1936.—Read 12 November, 1936.]

The "computable" numbers may be described briefly as the real numbers whose expressions as a decimal are calculable by finite means. Although the subject of this paper is ostensibly the computable *numbers*, it is almost equally easy to define and investigate computable functions of an integral variable or a real or computable variable, computable predicates, and so forth. The fundamental problems involved are, however, the same in each case, and I have chosen the computable numbers for explicit treatment as involving the least cumbrous technique. I hope shortly to give an account of the relations of the computable numbers, functions, and so forth to one another. This will include a development of the theory of functions of a real variable expressed in terms of computable numbers. According to my definition, a number is computable if its decimal can be written down by a machine.

In §§ 9, 10 I give some arguments with the intention of showing that the

Julia Robinson (1919–1985)

- Made major contributions to Hilbert's 10th problem.
- Introduced "JR Hypothesis".
- Final step was provided by Yuri Matiyasevich (aged 22).
- Robinson was President of American Mathematical Society (1983–1984) and first woman mathematician elected to US National Academy of Sciences.

WWII

- On September 4, 1939 Turing began his duty at the the Government Code and Cypher School at Bletchley Park.
- He worked on breaking German naval cryptosystems.
- Electronic computers were built at Bletchley Park for this purpose.
- Governments started to take cryptography and cryptanalysis very seriously.

1970s

- In the 1970s there was a mathematical revolution in cryptography, both in secret agencies and public domain.
- The notion of public cryptography, and new cryptosystems, were proposed by James H. Ellis, Clifford Cocks and Malcolm J. Williamson (at GCHQ) and Whitfield Diffie, Martin Hellman, Ralph Merkle, Ron Rivest, Adi Shamir and Leonard Adleman (various US institutions).

1985/1986

- Neal Koblitz and Victor Miller proposed elliptic curve cryptography.
- Elliptic curves are a class of Diophantine equations

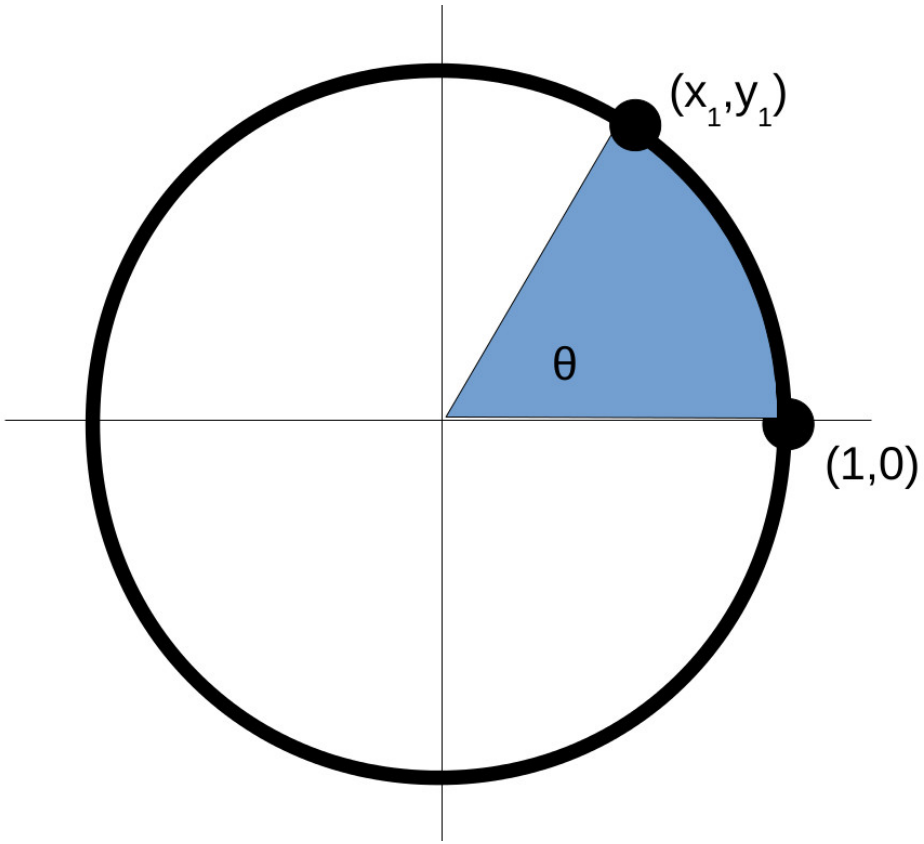
$$y^2 = x^3 + Ax + B$$

  that have been a major theme in number theory for over a century.
- The crux is that there is a mathematical problem (the elliptic curve discrete logarithm problem) that seems to be difficult for computers to solve.
- For the first time, Diophantine equations became part of applied mathematics, and hence political.

1985/1986

- Around the same time I started university at Waikato, to study computer science.
- I was mad about computers, and I had enjoyed maths at school due to my great teacher Bill Cooper.
- Heather Gardiner taught a 2nd year course in abstract algebra which I found inspirational.
- My honours thesis, supervised by Kevin Broughan, was on computational number theory.

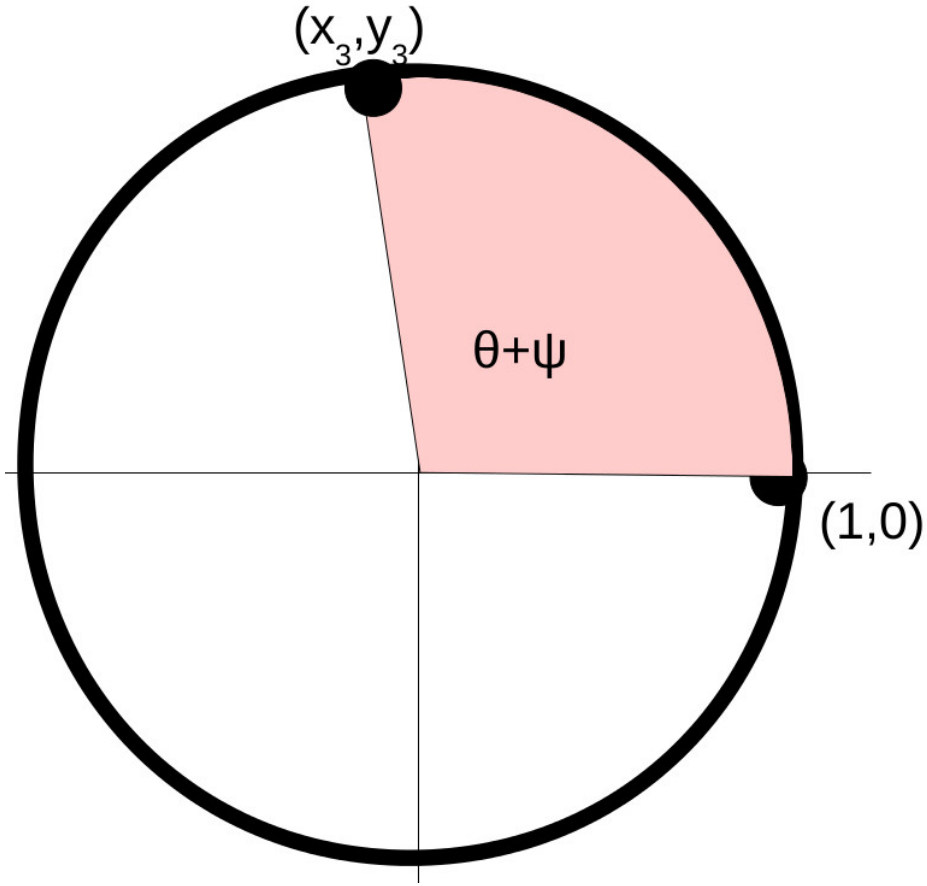
$$X^2 + Y^2 = 1$$



The circle group

- Let $(x_1, y_1), (x_2, y_2)$ be points on the circle.
- Each point defines an angle.
- The point $(1, 0)$ corresponds to an angle zero.
- (x_1, y_1) defines an angle θ and (x_2, y_2) defines an angle ψ.
- One can add the angles to get the angle $\theta + \psi$ and this gives a new point (x_3, y_3).

The point (x_3, y_3)



The circle group

- Let $(x_1, y_1), (x_2, y_2)$ be points on the circle.
- The point (x_3, y_3) corresponding to adding the angles is given by

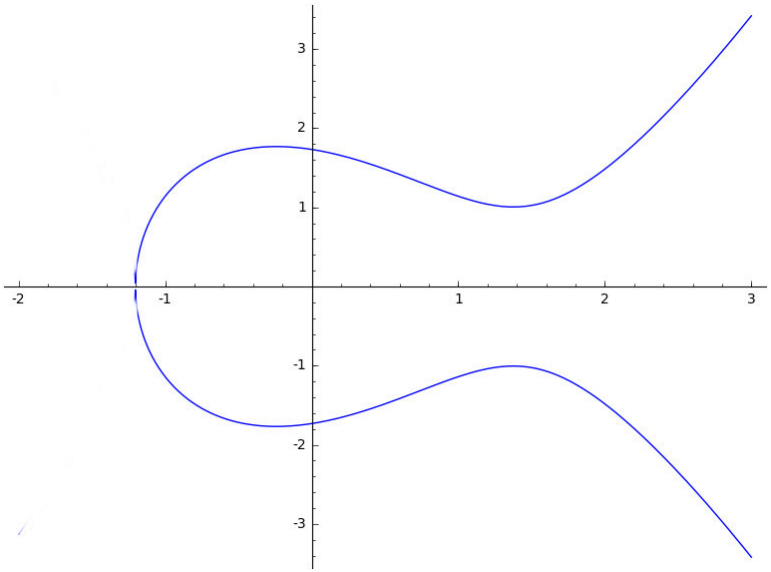
$$(\ x_1x_2 - y_1y_2 \ , \ x_1y_2 + x_2y_1 \ ).$$

- This is an example of an algebraic group.

Discrete Logarithm Problem

- Let (x_1, y_1) be a point on the circle.
- Suppose one adds the angle n times, where n is very large. Let (x_2, y_2) be the resulting point.
- Given (x_1, y_1) and (x_2, y_2) can you determine n efficiently?

Elliptic curves



- Not ellipses!
- Given by equation $y^2 = x^3 + Ax + B$.
- An algebraic group.
- Rich source of hard computational problems.

1990s

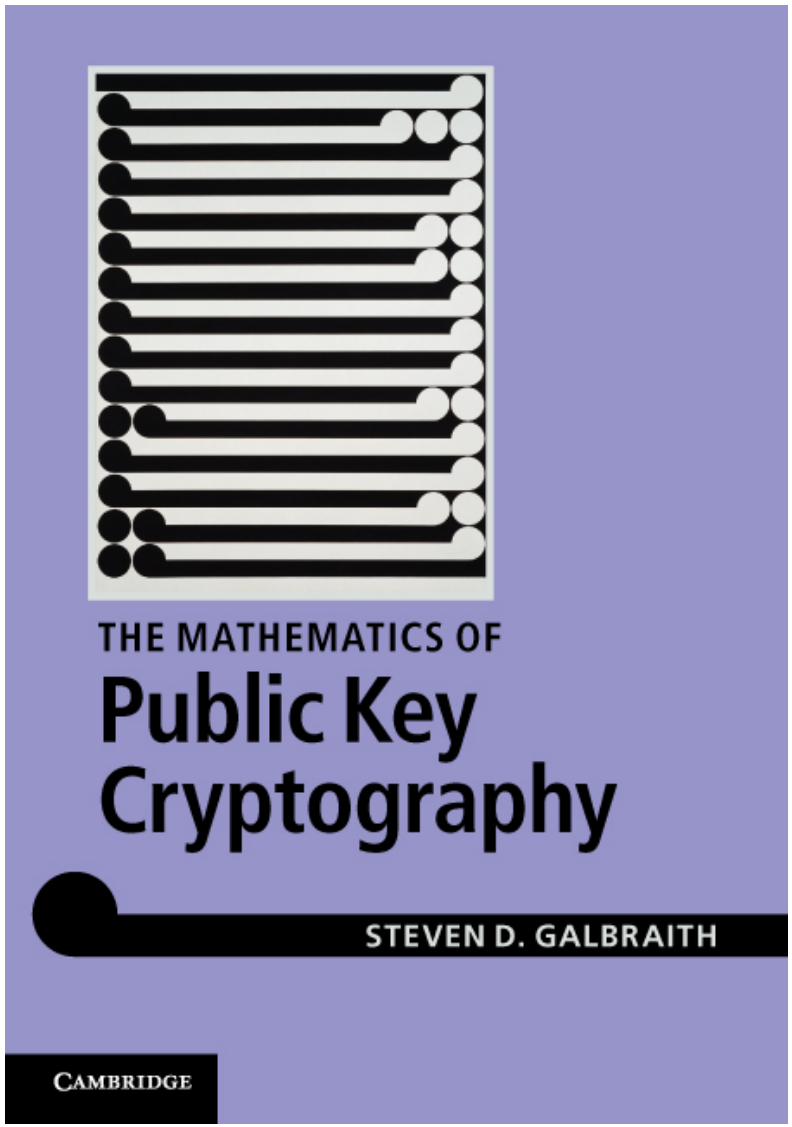
- PhD in Oxford, working on moduli spaces of elliptic curves.
- What was the point of my thesis?
- $(w, x, y, z) = (6, 8, -1, -2) \in X_0^+(311)$.
- I was lucky to find it.
- This special point corresponds to special elliptic curve that was previously unknown.

Career trajectory

- Royal Holloway University of London (UK), where I learned a lot from Simon Blackburn.
- University of Waterloo (Canada), mentored by Alfred Menezes.
- Institut für Experimentelle Mathematik (Germany), where I learned a lot from Hans-Georg Rück.
- University of Bristol for an annus mirabilis in 2000/2001.
- Back to Royal Holloway as a lecturer (2001-2009).
- Came home to Auckland in 2009.

Research

- My goal is always to bring clarity and simplicity to a subject.
- New algorithms for computational problems
- Efficient implementation of cryptosystems
- Cryptanalysis
- Fundamental question: Why are some computational problems hard?
- My other main contribution is in communication and knowledge transfer between pure mathematics and applications.


THE MATHEMATICS OF
Public Key
Cryptography
STEVEN D. GALBRAITH
CAMBRIDGE

The ellipticnews blog

ellipticnews.wordpress.com

Edward Snowden

- Leaked classified information from the National Security Agency (NSA) in 2013.
- Implied that US agencies had interfered with the public standardisation process for cryptographic algorithms.
- Example: Dual_EC_DRBG (an elliptic curve based pseudorandom bit generator).

Lasting value of my work?

- Elliptic curve cryptography is widely used:
  - Bitcoin
  - Supported in secure shell (SSH) and transport layer security (TLS)
  - Austrian Citizen Card
  - Sony PlayStation 3
- Is it possible to quantify the contribution of my own work to the success of ECC?
- One major threat on the horizon: Quantum computing.

Post Quantum Shift

- Elliptic curve cryptography is not secure against a quantum computer.
- In August 2015 the NSA announced they "will initiate a transition to quantum resistant algorithms in the not too distant future".

  > *Those partners and vendors that have not yet made the transition to Suite B elliptic curve algorithms, we recommend not making a significant expenditure to do so at this point.*

- In August 2016, NIST announced a formal Post-Quantum Crypto Standardization process

  `http://www.nist.gov/pqcrypto`

What to do when one's research area is threatened with obsolescence?

1. Deny
2. Ignore
3. Embrace

Ethical Responsibility

- I don't want to be the sort of person who obstructs progress.

  Science advances one funeral at a time

  – Max Planck /Neils Bohr/Carl Gauss
- I have an ethical responsibility to my students.
- It is not ethical to train students in a research area that limits their career options.
- So my current students are mostly working on post-quantum cryptography.

Ambitious goals for the future

- Talk less and listen more.
- Share.
- Support junior colleagues.
- Be a thorn in the side of senior administration.
- Not be part of the problem.

- Be a leading researcher in post-quantum crypto, break isogenies, invent new paradigm in lattice crypto, etc etc.

- So let Diophantine equations return to the paradise of pure mathematics, untainted by their application to information security, and let G. H. Hardy rest in peace.
- Ngā mihi maioha.