Cosc 412: Cryptography and security
Lecture 12 (30/9/2020)
Quantum computation

Michael Albert
michael.albert@cs.otago.ac.nz

The RSA trapdoor

Given a positive integer $N = pq$, which is the product of two large primes, p and q, Eve cannot find its prime factorisation.

A keyhole?

If P is a prime and

$$a^2 \equiv 1 \pmod{P}$$

then,

$$a \equiv \pm 1 \pmod{P}.$$

But, if N is composite then there are other solutions of

$$b^2 \equiv 1 \pmod{N}.$$

Given such a b:

$$\begin{aligned} b^2 &= kN + 1 \\ b^2 - 1 &= kN \\ (b-1)(b+1) &= kN. \end{aligned}$$

Then:

$$1 < \gcd(b-1, N), \gcd(b+1, N) < N$$

and so we would know some non-trivial factors of N.

Building a key

For composite odd N with at least two distinct prime factors, and x with $\gcd(x, N) = 1$ the following hold with probability at least $3/4$:

- The least positive integer r such that $x^r \equiv 1 \pmod{N}$ is even (called the *order* of x), and
- $x^{r/2} \not\equiv -1 \pmod{N}$.

So, if Eve had access to an *order finding algorithm* then she would have the ability to break RSA encryption.

Finding a factor of N

1. If N is even, return 2.
2. If $N = a^b$ for some $a, b \geq 3$ return a (see Note 1)
3. Randomly choose $2 < x < N - 1$. If $\gcd(x, N) > 1$ return it.
4. Compute the order, r, of x modulo N.
   - If r is odd, or $x^{r/2} \equiv -1 \pmod{N}$. Fail (see Note 2)
   - Otherwise, return $\gcd(x^{r/2} - 1, N)$.

Note 1: $b < \log_2 N$ in this case so this is easy to check classically.
Note 2: This occurs with probability at most 1/4, so actually just restart from (3).

Order finding on a quantum computer

- Let N be given, and choose n with $N < 2^n$.
- Consider a pure n-qubit state, $|b\rangle$ as representing an integer in the range $[0, 2^n)$.
- For $1 < x < N$ consider the map, defined as follows:

$$U|b\rangle = \begin{cases} |xb \pmod{N}\rangle & \text{if } b < N, \\ |b\rangle & \text{if } N \leq b \end{cases}$$

- Then U is unitary (easy to check) and we can compute it with polynomially many gates (a bit harder).

Eigenvalues and all that

Suppose that the order of x is r. Let $\omega = \exp(2\pi i/r)$. For $0 \leq s < r$ define:

$$|u_s\rangle = |1\rangle + \omega^s |x\rangle + \omega^{2s} |x^2\rangle + \cdots + \omega^{(r-1)s} |x^{r-1}\rangle .$$

Then

$$U |u_s\rangle = \omega^{-s} |u_s\rangle .$$

and

$$|1\rangle = |u_0\rangle + |u_1\rangle + \cdots + |u_{r-1}\rangle .$$

(Magic happens) Using a technique called *quantum phase estimation* we can arrange to get an output (on some new lines) that, with probability as close to 1 as we like, is a t-bit approximation to some s/r.

Back to the classical world

- The quantum computer has allowed us to compute a t-bit approximation to s/r for some s (randomly caused by quantum measurement stuff), but t under our control.
- Given a binary number, we can compute its “best” rational approximations using a technique called *continued fractions* – if $2r^2 \leq 2^t$ (i.e., basically if $t \geq 2n$) then we can *guarantee* that s/r will occur as one of them.
- After a bit of cleaning up (s/r might not be in lowest terms), we’ll have r (the cleaning up can be done in a way that requires us to run the algorithm only a constant number of times).

The practicality of quantum computing?

There are two fundamental issues that cause a gap between the ideal view of (gate-based) quantum computing and current experimental results:

fidelity The error rate of the various components of a QC. At present each two-qubit gate has an error rate of “a few percent”.

decoherence Since the QC cannot be completely isolated from the universe at large there will always be some interactions with the environment – effectively this can be thought of as the environment making small random measurements on the system which can (will) cause a partial collapse of the wave function.

Error correction

- Based on classical experience the obvious approach to the problems of (lack of) fidelity and decoherence would be to use *error correction*.
- But quantum error correction is a rather trickier beast! The error correction overheads are very high.
- With a 0.1% error rate per physical qubit, it would require approximately 15,000 physical qubits to provide *one* error-corrected logical qubit.

Quantum supremacy

- An often-heard phrase.
- What does it mean?
- From the NAS report:

> ***Finding****: While several teams have been working to demonstrate quantum supremacy, this milestone has not yet been demonstrated . . . . Its achievement will difficult to establish definitively, and this target may continue to move as improvements are made to classical approaches for solving the chosen benchmark problem.*

The killer apps?

- Quantum chemistry
- Optimisation (including machine learning)
- Defeating (some) cryptographic protocols
- From the NAS report:

  > ***Finding****: Quantum computers are unlikely to be useful as a direct replacement for conventional computers, or for all applications; rather, they are currently expected to be special-purpose devices operating in a complementary fashion with conventional processors, analogous to a co-processor or accelerator.*

Some final quotes

***Key Finding 1**: Given the current state of quantum computing and recent rates of progress, it is highly unexpected that a quantum computer that can compromise RSA 2048 or comparable discrete logarithm-based public key cryptosystems will be built within the next decade.*

Some final quotes

***Key Finding 3**: Research and development into practical commercial applications of noisy intermediate-scale quantum (NISQ) computers is an issue of immediate urgency for the field. The results of this work will have a profound impact on the rate of development of large-scale quantum computers and on the size and robustness of a commercial market for quantum computers.*