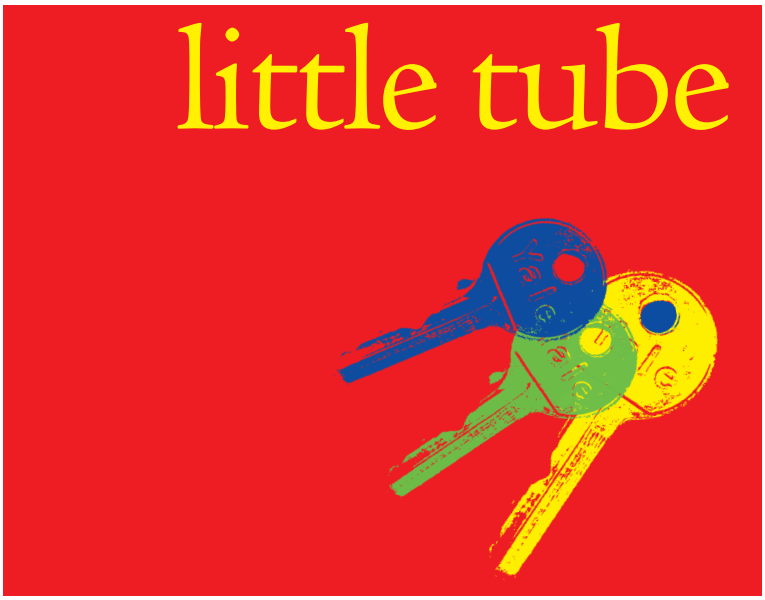
If the Twinkle machine takes off, the writing is on the wall for conventional cryptography.

Twinkle, Twinkle



There's a radically new kind of computer on the horizon. It's about the size of a bottle of whisky, computes with light, and cracks code in the twinkle of an eye.

The ultimate success of e-commerce rests on having rock-solid encryption, and the most promising technology is public-key cryptography. The idea is that everyone is issued with two keys: one is the 'public' key, freely announced; the other is the 'private' key, a closely guarded secret.

For example, if Alice wants to send a message to Bob, she looks up Bob's published public key, encrypts her message with it, and sends it to Bob. When Bob gets the message, he decodes it using his secret, private key. Anyone can send Bob a secure, encrypted message, but only Bob, who alone has the private key, can decode it.

What makes public-key encryption secure is the difficulty of figuring out the private key, given the public key. The two keys, each of which is a single, very large, number, have a special relationship, but untangling it is enormously hard. It boils down to a mathematical technique called factorisation: given a huge number, you have to find which two unique prime numbers, when multiplied, give the number.

One of the most popular public-key encryption methods today is the RSA system <www.rsa.com>. The 'S' of RSA is Adi Shamir, a computer scientist at the Weizmann Institute of Science in Israel <www.weizmann.ac.il>. Ironically, Shamir has just devised a new kind of computer that undermines the security of the system he helped to invent. He calls his machine 'Twinkle'.

No-one has built a Twinkle yet, but Shamir has published detailed plans. On the inside base of a light-tight cylinder will be a single wafer containing a few hundred thousand processing cells. Each cell will house two small memories, a photoreceptor, and a gallium arsenide light-emitting diode (LED).

Twinkle clocks at 10GHz, about 20,000 times faster than today's fastest PCs, and at speeds like this, electrical pulses simply can't travel around electrical circuits fast enough. Instead, Twinkle uses an optical clock: mounted on the inside top of the cylinder is a bright LED, shining down onto the wafer below. It flashes once every 10 thousand millionths of a second. The photoreceptor in each cell responds to the flash, and the cell performs a computation, trying to factor the number it's working on. The cell's LED flashes if it succeeds, and each flash is recorded by another photoreceptor mounted at the top of the cylinder.

Does this mean that RSA is seriously undermined? No. RSA responded rapidly, stating that Twinkle would only be capable of cracking the simpler versions of RSA coding. Increase the number of bits in the RSA codes, and Twinkle is quickly foxed.

Nevertheless, some experts think the writing is on the wall for conventional cryptography. Researchers at Los Alamos National Labs <qso.lanl.gov/qc> are exploring new techniques based on quantum physics. 'To break quantum encryption, a cracker will first have to break the laws of physics,' says Dr Richard Hughes, director of the Los Alamos programme.

Mounted on the inside top of the cylinder is a BRIGHT LED, SHINING DOWN onto the wafer below. It flashes once every 10 thousand millionths of a second

We don't have quantum encryption yet, but when we do, it really will be safe to send your credit card details across the internet. Probably.

TOBY HOWARD