The Quest for the Uncrackable Code

Vol. 11 Issue 05

A new star recruit at the University of Calgary is using quantum physics to develop perfectly secure electronic transactions. The business world is watching

By Will Gibson

Dr. Wolfgang Tittel invites you to imagine a box, smaller than small.

Smaller than any atom.

So small, in fact, that you can never tell for certain if it's in one spot or another...or both

The box is wired to a tiny grenade, set to blow if it's tampered with. Any microscopic burglar bent on robbing the contents would find himself holding a handful of ash. The lock is impregnable. If you don't have the key, you aren't getting in.
And someday soon -- 15 years, maybe 10, maybe less -- we could be putting every secret we own in such tiny boxes. Everything from military and state secrets to medical information, the formula for Coca-Cola or the credit card number you used to buy your mother a birthday gift. The box will hold those secrets forever in perfect security, until the owner comes along with the key.

The box is made of nothing but light, and the secrets it will carry will be written on the fabric of reality itself.

Baffled? You're in good company. Even Albert Einstein had trouble wrapping his mighty brain around quantum physics, that troublesome branch of science which studies matter on a subatomic level, where particles can be both points and waves, and occupy multiple states and positions at the same time, and where nature is fundamentally unpredictable and fluid. "I, at any rate, am convinced that He [God] does not throw dice," Einstein said.

Even Tittel, a new star hire for the University of Calgary who's been studying this

stuff since he was a grad student back in Geneva, finds the mushy nature of quantum reality annoying. “Of course it bugs me. Understanding is just the process by which we link the known to the unknown. We have this quantum theory that seems to contradict common sense. If you can observe it working in the lab, and find a practical way to use it, it starts to bother you a lot less.”

That emphasis on the practical was what drew Tittel to advanced physics in the first place. He was born in Paris, the child of German intellectuals. His father was a physicist, specializing in optics. “I remember asking him how a laser worked. The explanation he gave me was wrong... I think he did that deliberately,” he says, laughing. “He knew I’d try to build one. Seven-year-old boys should not build working lasers.”

He’s 37 now, and his academic career has spanned the birth and first steps of a new science, quantum cryptography, from experiments in 1992 to early commercial applications in 2007. “The commercial applications are going to drive this science,” he says. “It’s been estimated that the quantum encryption market has the potential to be worth $3 billion by 2015. I’m confident this technology will be part of our communications system in just a few years.”

In contrast to existing electronic encryption, which encases data in computer-generated, mathematical formulas that are extremely difficult but never impossible to crack, quantum encryption is based on “quantum indeterminacy,” the notion that so irritated Einstein. Subatomic particles are said to be “indeterminate” because the act of measuring them -- of finding out where they are and where they’re going -- changes the aspects being measured. In the everyday world, things are in one place or another. In the quantum world, they’re said to be “superpositioned” --
in many places at once -- until they’re measured. It’s known as the “observer effect” -- at a fundamental level, reality is a blur.

Tittel’s work offers a pretty good primer in the observer effect. Let’s say two people -- Jack and Jill -- want to exchange a message secretly. Instead of picking up the phone, Jack sends Jill a series of photons -- light particles -- down a fibre-optic line. The particles are polarized into one of two positions: rectilinear (horizontal or vertical) or diagonal (45 degrees to the left or right of vertical). Depending on how the particles are oriented, they represent either a 0 or a 1 in the digital code “key” Jack is sending Jill. Jack sends Jill his key by encoding the photons randomly in either the rectilinear or diagonal mode. Jill decides to measure the photons in one mode or the other. She can’t use both.

On average, Jill will accurately decode about half of the key. She can then call up Jack on an unsecured line and tell him how she measured the incoming bits of information – as long as she doesn’t reveal her results, the key stays secure. Then Jack tells Jill which of the incoming photons were measured correctly.

Once they’ve exchanged the key, they can send secure messages. What makes the system spy-proof is that anyone intercepting the key ends up with gibberish – because the eavesdropper doesn’t know which of the two methods were used to encode the individual bits of the message. Even better, when the eavesdropper tries to send the key on to Jill to cover his tracks, he introduces errors that Jack and Jill will spot, alerting them to the attempt to break the code and the need to come up with a new key.

In short, you can’t break a quantum code without breaking a bedrock law of physics, and you can’t even try without blowing your cover. That’s how it works in theory. In practice, it’s a lot more awkward.

For starters, the single-file stream of encoded photons that make up a quantum key can’t travel very far before it falls apart. Tittel himself set a distance record back in Geneva for sending a quantum code transmission via optical fibre line – a transmission that travelled just 11 kilometres. “You can’t boost the message the way you would with an electrical signal, because that’s a form of copying. And copying the quantum code destroys its content,” explains Raymond Laflamme, director of the Institute for Quantum Computing at the University of Waterloo. “We need a form of quantum error correction that would make the signals more robust. We don’t have that yet.”

The transmission rate is also extremely slow and costly. “Basically you can only send yes-no answers right now,” says Barry Sanders, director of the Institute for Quantum Information Science at the University of Calgary, where Tittel assumed the newly created iCORE/General Dynamics Canada Industry Chair in Quantum Cryptography and Communication in April. “Remember that ‘cone of silence’ gadget on that old TV show, Get Smart? It was very high-tech, but they couldn’t hear each other talk when it was on. That’s basically where quantum cryptography is now.”

So quantum cryptography is a boutique item at the moment, too expensive and limited for wider commercial applications. The American firm MagiQ Technologies offers a fibre-optic system for $70,000 to $100,000 US. Some observers doubt whether the technology has any immediate uses outside the lab. “I’d call it Utopian. A large-scale network simply isn’t possible right now,” says Osmar Zaiane, associate professor of computing science at the University of Alberta.

The people working to make quantum encryption pay believe their first customers will be large institutions needing elaborate security, like banks and armies. The Internet itself started out as a project of Pentagon-backed researchers. It’s no accident that the co-sponsor of Tittel’s chair at the U of C is the military contractor General Dynamics Canada. “You can see the battlefield applications already – counter-intelligence, transmitting troop movements,” says Sanders.

But where’s the wider commercial market? E-commerce could always use the kind of marketing boost an unbreakable system of communication could provide. We’re getting more comfortable with the idea of buying things online; Statistics Canada reported Canadian companies and individuals purchased almost $8 billion worth of goods and services via the Internet in 2005, a quantum leap from the $3 billion in sales reported in 2003. (The 2003 survey, it should be noted, measured household purchases.) A little more than half of home surfers used the ’net to do banking and pay bills in 2005. The West is leading the rush to online retail: 45% of adult users in Alberta and British Columbia bought through a browser in 2005. Internet use among adults in Alberta hit 71% that year – 77% in Calgary and 69% in Edmonton –
topping the 68% national average.

But there’s still a lot of anxiety out there in the virtual marketplace. Eight in 10 Canadians told an Industry Canada survey in 2005 that they were concerned about privacy and security on the Internet. So far, that hasn’t slowed down those already using the Web to buy and bank; 72% of those surveyed said their security concerns hadn’t affected their actual Internet use. But worries about electronic fraud and identity theft – driven by recent high-profile cases like the hacker attack on customer databases at the Winners and HomeSense retail chains – may be making technophobes even more wary of passing their credit-card numbers to virtual strangers.

“The sheer scope of these large-scale information thefts rattles a lot of people,” says Rebecca Grant, associate professor of information systems at the University of Victoria business faculty. “A lot of people who are frightened of Internet buying think nothing of giving their credit-card number over the phone. But the promise of [unbreakable encryption] would corner the market completely.”
The real problem, say a lot of people working in e-business, is that most electronic fraud involves old-fashioned human error – or greed. Someone tosses a pile of unshredded loan applications in a garbage dumpster, someone leaves a laptop unattended, someone boosts and duplicates credit cards, and suddenly you have a crime spree. Seldom does this priceless personal data seem to get diverted while it’s racing through wires or empty space.

“The real security problem isn’t transmission. It’s storage,” says Ashif Mawji, CEO of Edmonton-based Upside Software. “Many small merchants still don’t store this information properly, using a third-party data storage firm like PayPal. It always seems to be the human element that falls down.”

Maybe so. But there’s another argument working in quantum encryption’s favour: the technology is going to make itself inevitable.

Encryption is only one angle of quantum information science. Around the world, physicists – including some at the U of C –are racing to build a practical “quantum computer,” a machine which would use the power of superposition to solve problems at a speed which would make the fastest computer currently in existence look like it was unplugged. Right now, encryption depends on very complex mathematical problems that take too long for a conventional computer to crack. None of those “classical” encryption systems would be able to stand up to a quantum computer. Once quantum computing gets rolling, every coded secret on the planet will be up for grabs – except the ones protected by a quantum code.

“One has to consider encoded commercial or military information which may be held in the wrong hands now, by people waiting for the technology to emerge to break the encryption,” says Laflamme. “Those codes will be vulnerable in just 15 or 20 years’ time. We have to start thinking about these things now.

“It’s hard to estimate how fast quantum information technology will spread. You might remember that Popular Mechanics prediction in 1949, that computers would

someday be so advanced they would only weigh about a ton each. Once we solve the error correction problem, this technology will spread very fast."

And that, says Laflamme, is about the only thing you can predict about this most unpredictable technology: "Eventually, it will be everywhere."
