CALGARY HERALD SINCE 1883

ARCHIVE STORY
List of the 7 Days Archived & Search Tools

SUNDAY, FEBRUARY 13, 2005

SECTIONS IN THIS ISSUE:
News | City & Region | Opinion | Letters | Observer | Faith & Reason | Sports | Entertainment | Taste | Real Life | Business on Sunday | Life at Home

The code that can't be cracked

Quantum physics will alter the Internet -- for better or worse

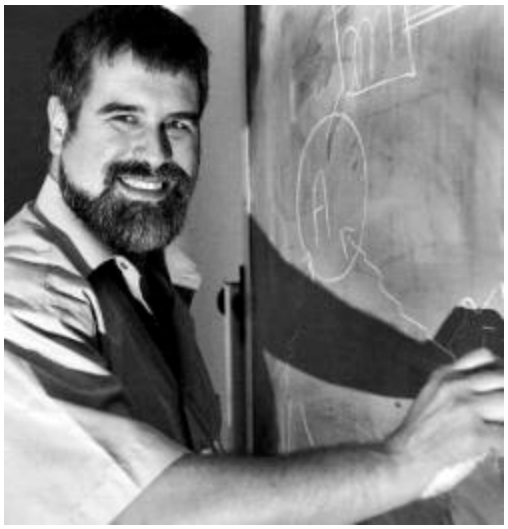
Alison MacGregor
CanWest News Service

February 13, 2005

It began 25 years ago in the warm coastal waters of Puerto Rico when a stranger swam over to Gilles Brassard and struck up a conversation about using quantum physics to make banknotes impossible to counterfeit.

"I had no idea who he was," recalled Brassard, then a 24-year-old prodigy and computer-science professor at the Universite de Montreal. "He just started talking nonsense about quantum physics."

The stranger turned out to be U.S. physicist Charles H. Bennett. Their chance meeting while attending a



CREDIT: Marie-France Coallier, CanWest News Service

Experts fear the ability to send unbreakable coded messages -- as developed in part by Universite de Montreal quantum physics teacher Gilles Brassard

Services

Calgary city site
CLICK HERE

Calgary city site
Calgary Herald
Global Calgary
Calgary Flames
Stampeders
Hitmen
Roughnecks
Event Listings
Sports Events
Live Music
Movies
Restaurants
Bars
Contests
Sound Off!

tonight on Global
7:00 PM
Train 48
7:30 PM
Entertainment Tonight
8:00 PM
Las Vegas
9:00 PM
Fear Factor
10:00 PM
24

full listings: TVtimes

theoretical computer science conference would end up revolutionizing the art of code making, also known as cryptography.

Together, Brassard and Bennett would go on to found a field of science -- quantum information processing -- whose effects on society some say could even rival the impact that the steam engine had in its time.

Already, experts agree, Brassard and Bennett's most famous invention, a technique known as quantum cryptography, is set to eliminate terrifying vulnerabilities that could soon arise in the way governments, banks, the military, business and the public use computers and the Internet to communicate and store data.

Some observers see the technology as one day making the Internet secure enough that medical professionals could share confidential health data online in ways that would be insecure now.

Yet, for all its promise, this invention is also making governments nervous.

The ability to send unbreakable coded messages could just as easily be exploited, authorities fear, by criminals and terrorists who now lack a foolproof way of avoiding having their messages cracked.

In the midst of all this excitement and controversy is Montreal-based Brassard, who has made Canada a world leader in his fast-growing field.

Because of him, Canada "has turned out to be the best place in the world" to do research in quantum information processing, says physicist Raymond Laflamme, a leading figure in the field who recently returned to Canada from a post with the U.S. Department of Energy's Los Alamos National Laboratory, Canada.

"All of this is thanks to Gilles," he says.

Barry Sanders, a quantum physicist who recently returned to Canada from a research post in Australia, agrees, saying Brassard has played a key role in making this country "the world leader in this field."

Brassard's and Bennett's invention sprung from their discovery of how principles from the previously unlinked fields of quantum physics and computer science could be combined to establish an unbreakable secret key.

Instead of transmitting information along cables via electronic signals, they use polarized photons -- tiny particles of light -- which are so sensitive that, when intercepted, they immediately become corrupted. This renders the message unintelligible and tips off both sender and intended recipient to the spying attempt.

What's causing particular excitement now is the way applications of Brassard's and Bennett's technology have just been commercialized and put to market.

Since late 2003, consumers have been able to acquire quantum cryptographic systems that make short-haul computer links unbreakable to spies. The systems are being sold by two competitors in Geneva and New York for as little as $70,000 US. Both firms' devices use Brassard and Bennett's seminal insight.

More...

Print Story Send to a Friend

SUNDAY, FEBRUARY 13, 2005

SECTIONS IN THIS ISSUE:

Monday, February 14, 200!

CALGARY HERALD

SINCE 1883

WEATHER
-7°
Fair
FORECAST OTHER CITIES

ARCHIVE STORY

List of the 7 Days Archived & Search Tools

SUNDAY, FEBRUARY 13, 2005

SECTIONS IN THIS ISSUE:

News | City & Region | Opinion | Letters | Observer | Faith & Reason | Sports | Entertainment | Taste | Real Life | Business on Sunday | Life at Home

The code that can't be cracked

...Continued

But that's only a start, says Laflamme. "The potential is absolutely enormous." Today's most sophisticated codes used for the protection of information on computers rely on hugely complex mathematical calculations that present-day computers aren't believed to be powerful enough to solve.

Yet, as Brassard explains, it's possible someone has already figured out how to crack these codes. If so, such a person might want to keep this quiet so as to benefit personally, Brassard remarked, although there could also be an altruistic reason for doing so.

The reason? "Society would collapse, electronic commerce would collapse," Brassard said. "There would be chaos. I would keep quiet -- just as I would if I found a new weapon of mass destruction."

But the biggest fear in the cryptographic world is that a new kind of super-powerful "quantum computer" could soon be constructed that would have the capacity to quickly solve the kinds of code-breaking problems that today's computers are stumped by.

Already, experts say, a U.S. mathematician, Peter Shor, has developed a formula that could be used by a quantum computer, once one has been built,

Services

Calgary city site
CLICK HERE

Calgary city site
Calgary Herald
Global Calgary
Calgary Flames
Stampeders
Hitmen
Roughnecks
Event Listings
Sports Events
Live Music
Movies
Restaurants
Bars
Contests
Sound Off!

tonight on Global
7:00 PM
Train 48
7:30 PM
Entertainment Tonight
8:00 PM
Las Vegas
9:00 PM
Fear Factor
10:00 PM
24

full listings: TVtimes

to crack current encryption technology.

The prospect of such a computer being constructed obviously worries governments, business and the military -- and should be of concern to all who value their privacy.

It would be "a nuclear bomb to the Internet," says Barry Sanders, director of the University of Calgary's Institute for Quantum Information Science. "All of the security that we rely on when we use the Internet would be obsolete."

And this is why Brassard and Bennett's invention is causing such a stir: theirs is the first practical form of cryptography that could not be broken, even by some yet-to-be-built quantum computer.

The key to the security of a quantum cryptography code, Laflamme explains, is that it "does not involve solving a mathematical problem; it would involve breaking the laws of physics."

So promising is the field of quantum information processing that governments and corporations around the world are investing millions of dollars in research in the field.

The first-ever local quantum-encrypted network of computers is now up and running in Cambridge, Mass., where it is managed by the pioneering Internet firm BBN Technologies Inc.

And the Los Alamos National Laboratory's quantum cryptography team has teamed up with six European research institutions to push the field further. In December, the team tied with another group to snag one of the world's most prestigious science prizes -- the European Union's $1.3-million US Descartes research prize -- for its project to build a secure global quantum cryptographic communications system.

In Canada, Research in Motion founder and co-chief executive Mike Lazaridis put up $100 million of his own money in 1999 to fund the non-profit and independent Perimeter Institute of Theoretical Physics in Waterloo, now a leading centre of quantum information research. (Two more RIM executives have since contributed another $20 million, while Ottawa and Ontario have kicked in another $54 million.)

More...

Print Story Send to a Friend

SUNDAY, FEBRUARY 13, 2005

SECTIONS IN THIS ISSUE:
News | City & Region | Opinion | Letters | Observer | Faith & Reason | Sports | Entertainment | Taste | Real Life | Business on Sunday | Life at Home

List of the 7 Days Archived & Search Tools

Search canada.com About Us Advertise Site Map Privacy Terms FAQ Our Partners

CLASSIFIEDS
- Find a job
- Find a car
- Find a home
- Obituaries
- Shopping
- Personals
- Find an ad
- Place an ad

IN THE HERALD
News
The Editorial Page
Letters
City & Region
Entertainment
Calgary Business
Real Life
Sports
Newspaper Ads
Weekly Sections:
- Driving
- Faith & Reason
- Life at Home
- New Homes
- New Condos
- Neighbours
- Observer
- Taste
- Travel
Columnists
Headline Scan
Online Extras
Sound Off!
7-Day Archive
Appointment Notices
ELECTRONIC EDITION

YOUR HERALD
Subscribe
Help
Send us a news tip
Letters:
- To the editor
- About your event
- Site Feedback
Advertising
About Us
Contact Us
Services

ARCHIVE STORY
List of the 7 Days Archived & Search Tools
SUNDAY, FEBRUARY 13, 2005
SECTIONS IN THIS ISSUE:
News | City & Region | Opinion | Letters | Observer | Faith & Reason | Sports | Entertainment | Taste | Real Life | Business on Sunday | Life at Home

The code that can't be cracked

...Continued

Last month, the University of Calgary got into the act, launching its Institute for Quantum Information Science.

There have been commercial developments too.

In 2003, a Swiss firm, id Quantique SA of Geneva, became the first to sell a quantum cryptography system to the public. Another company, New York City's MagiQ Technologies Inc., soon followed.

Yet Brassard and Bennett haven't made a penny from these ventures; they've chosen not to patent their discovery in the hopes of fostering an environment where colleagues can feel unhindered in their efforts to develop the field.

Other companies with projects in the works include IBM -- where Bennett is a research fellow at the company's Yorktown Heights, N.Y., research centre -- and Japanese computing giants NEC, Fujitsu and Toshiba.

So great is the interest among potential buyers that industry analyst Martin Illsley predicts the technology will be widespread in business and government settings in as little as five years.

Early adopters will likely be financial institutions, governments and telecommunications firms, said Illsley, an associate partner at consulting firm Accenture Inc., in a telephone interview from France.

Others share that optimism. In a report, International Data Corp. has predicted the market for quantum cryptography products will be about $30 million US within three years -- and about $300 million within 10 years.

Further reading:

- Bennett, C. H., Brassard, G. and Ekert, A. K., Quantum cryptography, Scientific American, October 1992, pp. 50 to 57.

- Stix, G., Best-Kept Secrets, Scientific American, January 2005, pp. 78 to 83.

- Singh, S., The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, Random House Inc., 1999.

Websites:

- Gilles Brassard -- http://inexistant.net/Gilles/index.html

- Charles Bennett -- http://www.research.ibm.com/people/b/bennetc/home.html

- Claude Crepeau -- http://www.cs.mcgill.ca/ 7/8crepeau/

- Raymond Laflamme -- http://www.iqc.ca/people/rlaflamme/

- Barry Sanders -- http://qis.ucalgary.ca/ 7/8bsanders/

Print Story Send to a Friend

SUNDAY, FEBRUARY 13, 2005

SECTIONS IN THIS ISSUE:
News | City & Region | Opinion | Letters | Observer | Faith & Reason | Sports | Entertainment | Taste | Real Life | Business on Sunday | Life at Home

List of the 7 Days Archived & Search Tools

Search canada.com About Us Advertise Site Map Privacy Terms FAQ Our Partners