ATTACHMENT 2: Profile and Detailed Achievements of the Group B Recipients of the 2022 C&C Prize

Dr. Charles H. Bennett

Current Position:
IBM Fellow, IBM Research

Personal History (born in 1943):

1964	BS in Chemistry from Brandeis University
1971	PhD from Harvard University
1971	Researcher, Argonne National Laboratory
1972	IBM Research
1995	IBM Fellow, IBM Research

Major Awards:

1995	IBM Fellow
1997	National Academy of Sciences (NAS) Member
1998	APS(American Physical Society) Fellow
2006	Rank Prize for Optoelectronics
2008	Harvey Prize
2010	Okawa Prize
	Thomson Reuters Citation Laureate
2012	Thomson Reuters Citation Laureate
2017	Dirac Medal of the ICTP
2018	Wolf Prize in Physics
2019	Micius Quantum Prize
2019	BBVA Foundation Frontiers of Knowledge Award in Basic Sciences
2020	Claude E. Shannon Award
2022	Breakthrough Prize in Fundamental Physics

Prof. Gilles Brassard

Current Positions:
Professor of Computer Science, Université de Montréal
Turing Chair for Quantum Software, QuSoft

Personal History (born in 1955):

1979	PhD. in Computer Science from Cornell University
1988	Full Professor, Université de Montréal
2001	Canada Research Chair

Major Awards:

2000	Prix Marie-Victorin

2006 Rank Prize for Optoelectronics
Fellow, International Association for Cryptologic Research
2010 Gerhard Herzberg Canada Gold Medal
2011 Killam Prize in Natural Sciences
2012 Thomson Reuters Citation Laureate
2013 Fellow, Royal Society of London
2018 Wolf Prize in Physics
2019 Micius Quantum Prize
2019 BBVA Foundation Frontiers of Knowledge Award in Basic Sciences
2022 Breakthrough Prize in Fundamental Physics

Achievements

Cryptography is one of the fundamental technologies that protect the security of information. However, most current cryptographic techniques, including those used in electronic commerce, are only computationally secure. In particular, they will become decipherable when quantum computers are put into practical use. This may also occur with the discovery of new algorithms, even for classical computers. The inability to detect the presence of eavesdroppers, as well as the possibility to harvest currently indecipherable messages now and decrypt them later, is a significant weakness, which it would be advisable to remedy in the network of the future. For this reason, quantum cryptography, introduced by Dr. Bennett and Prof. Brassard, is attracting attention as a cryptographic technology whose present and future security is guaranteed by the laws of physics.

The story begins in 1968-70 when Stephen Wiesner (deceased in 2021), then a graduate student at Columbia University, discovered some of the fundamental notions underlying quantum information: quantum banknotes, quantum multiplexing (a quantum implementation of what was later called oblivious transfer), and superdense coding. He made little effort to publish these ideas but circulated them in manuscript and discussed them with colleagues including Dr. Bennett and later Prof. Brassard. At the urging of his colleagues, his 1968 ideas were finally published in 1983 and the rest in 1992 with Dr. Bennett as co-author.

Before the work of Dr. Bennett and Prof. Brassard, who met in 1979, the only unconditionally secure way to send a secret message was the "one-time pad", which requires the users to agree beforehand (e.g. by meeting in person) on a shared secret (or "key") as long as the message they wish to transmit. Once used, as the name suggests, the key cannot be safely reused. Based on Wiesner's seminal but impractical notion of unforgeable quantum banknotes, Dr. Bennett and Prof. Brassard invented quantum key distribution (QKD), the first and now most widely practiced form of

quantum cryptography. Their so-called BB84 protocol allows two users, communicating by a quantum channel subject to eavesdropping (e.g. an optical fiber or free space optical path) and an unjammable public channel, to agree on a shared secret key, or to conclude that there has been too much eavesdropping for them to do so safely. If the key establishment succeeds, the users can use their key as a one-time pad for unconditionally secure communication. Though an eavesdropper can force the protocol to abort, they cannot, except with negligible probability, trick users into agreeing on a key that is not secret. This discovery was made possible by the confluence of physics (Dr. Bennett) and computer science (Prof. Brassard), a true example of interdisciplinary research.

In 1989 Dr. Bennett and Prof. Brassard, with their students Bessette, Salvail and Smolin, built the first working implementation of BB84, incorporating novel techniques for maintaining security in the presence of optical misalignment and detector noise. This was only a proof of principle, working over a distance of 32 centimeters, but in the 21st century the range of quantum cryptography has been increased to hundreds of kilometers through optical fiber and thousands of kilometers through satellites in space.

In addition to quantum cryptography, Dr. Bennett and Prof. Brassard, together with various collaborators, laid the foundation for the thriving science now called quantum informatics or quantum information theory. In 1993, with Crépeau, Jozsa, Peres, and Wootters, they discovered quantum teleportation, in which prior shared quantum entanglement enables users to transmit quantum information over a classical channel by disembodying an unknown quantum state at the sender’s end of a channel and reincarnating it at the receiver’s end with the necessary help of a classical message from the sender. Entanglement may thus be viewed as a stronger analogue of a shared secret key. Neither has any communications capacity by itself, but a shared secret key enables private communication via a public channel, while shared entanglement enables quantum communication via a classical channel. It is even possible to teleport entanglement itself, so that someone who is entangled with two other parties can establish entanglement between them using only classical communication, a process known as entanglement swapping.

Dr. Bennett and Prof. Brassard’s 1995 paper with Bernstein and Vazirani provided evidence that quantum computers cannot exponentially speed up general search problems; barring unexpected developments in the P=NP problem, Grover's 1994 quadratic speedup is the best that can be hoped for. With Shor, Popescu, and others they launched the quantitative theory of entanglement as a resource that can aid quantum communication and computation despite having no communication capacity by itself. In particular, they and colleagues discovered entanglement distillation, which

enables the establishment of near perfect entanglement from a larger supply of noisy entanglement.

They have also made important discoveries, sometimes with other collaborators, while not working together. For instance, Dr. Bennett and collaborators, generalizing the equivalence of quantum and classical communication in the presence of shared entanglement, proved the quantum reverse Shannon theorem, according to which all quantum channels of nonzero classical capacity can simulate one another efficiently in the presence of appropriate entanglement resources. Prof. Brassard's other discoveries with collaborators include quantum pseudotelepathy and the first theoretical circuit to achieve quantum teleportation.

Though the two branches of classical informatics–computation and communication–were developed separately by Turing and Shannon, they have become intimately connected in practice: almost every piece of communications equipment involves computation and vice versa. During the 21st century the two have been further integrated with cryptography and rebuilt on a common quantum foundation, which treats a classical channel as a quantum channel with an eavesdropper, and a classical computer as a quantum computer with an eavesdropper on each wire.

For their invention and development of quantum cryptography and their role in founding the field of quantum information science, Dr. Bennett and Prof. Brassard are well deserving of the C&C Prize.