Quantum Information Processing: The Good, the Bad and the Ugly

Gilles BRASSARD *

Université de Montréal, Département d'informatique et de recherche opérationnelle
C. P. 6128, Succursale Centre-Ville, Montréal (Québec), CANADA H3C 3J7
email: brassard@iro.umontreal.ca

Abstract. Quantum mechanics has the potential to play a major role in the future of cryptology. On the one hand, it could bring to its knees most of the current trends in contemporary cryptography. On the other hand, it offers an alternative for the protection of privacy whose security cannot be matched by classical means.

God only knows
God makes his plan
The information's unavailable
To the mortal man

— *Paul Simon*

1 Good or Bad? It's a Matter of Perspective

Following pioneering work by Paul Benioff [2], the idea that quantum mechanics could be harnessed to the cause of computational speed was planted by Richard Feynman [15, 16] in the early eighties and championed by David Deutsch [13] shortly afterwards. At least in principle, a quantum computer working on a few thousand quantum bits of memory can quickly perform an amount of computation greater than possible with a classical computer the size of the Earth running for the lifetime of the universe. Nevertheless, quantum computing was but a fringe pursuit for more than a decade because (1) building a quantum computer seemed totally out of reach from current and foreseeable technology, and (2) nobody knew of a *practical* computational problem that quantum computers could solve faster than classical computers.

This all changed in 1994 when Peter Shor made his momentous discovery: quantum computers can factor large numbers and extract discrete logarithms in expected polynomial time [21]. Even better—or worse, depending on the perspective—the time needed to factor an RSA integer [20] is in the same order as the time needed to use that same integer as modulus for a *single* RSA

* Research supported in part by NSERC, FCAR and the Canada Council.

encryption. In other words, it takes no more time to break RSA on a quantum computer (up to a multiplicative constant) than to use it legitimately on a classical computer [8]! Of course this has no practical consequences as long as quantum computers remain the stuff of dreams [18], but Shor's breakthrough gave a remarkable boost to the quest for understanding better the feasibility of quantum computation. In just a few years, this has lead to encouraging advances in the experimental manipulation of quantum information [19]. Although large-scale quantum computations—such as the factorization of a two-hundred digit number—are still rather speculative, nontrivial quantum computations involving perhaps as many as 10 or 20 quantum bits are on the horizon. Perhaps the most exciting recent discovery in quantum information theory is that of quantum error correction [19], which makes it theoretically possible to compute reliably with unreliable components.

Even if large-scale quantum computers—or perhaps special-purpose quantum factoring devices—become a reality, this would not doom all of classical cryptography. (Of course, "classical" is used here to mean non-quantum, and it includes secret-key and public-key cryptography on the same footing, just as "classical physics" lumps together Newton's mechanics with Einstein's relativity.) For one thing, quantum computing does not weaken information-theoretic secure schemes such as the one-time pad. Actually, it makes such schemes all the more important since they could remain the only safe alternative for classical cryptography. Not even all of public-key cryptography is threatened by quantum computing: it has been argued [3] that strong one-way functions that can be computed efficiently with classical computers but cannot be inverted efficiently even with a quantum computer may well exist. This would suffice to achieve computationally secure cryptographic pseudorandom generation, bit commitment schemes and zero-knowledge protocols for all of **NP**. Even though most public-key cryptosystems currently in use are based on the presumed difficulty of either factoring large numbers or extracting discrete logarithms, which would not survive widespread use of laptop quantum computers, alternative quantum-resistant public-key systems are not ruled out to the best of our current knowledge.

Shor's algorithms are not directly relevant to the security of secret-key cryptosystems such as the DES, *provided users do not establish their secret session key with public-key techniques* such as the Diffie–Hellman key distribution scheme [14]. However, a more recently discovered quantum algorithm, due to Lov K. Grover [17], could have an impact on the security of secret-key systems by significantly speeding up exhaustive search. For example, given a single matching pair of plaintext/ciphertext, single-key DES encipherment can be broken after a mere 185 million expected quantum encipherments of the known plaintext when the solution is unique [6, 10]. This number is admittedly large, yet it is hundreds of millions of times smaller than the $2^{55} \approx 3.6 \times 10^{16}$ expected number of DES encipherments required by classical exhaustive search. It is still an open question whether or not a quantum computer could break double-key encipherment of classical cryptosystems faster than a classical computer that uses the meet-in-the-middle attack.

A new application of Grover's algorithm was recently discovered in collaboration with Peter Høyer and Alain Tapp [12]: there is a quantum algorithm that finds collisions in arbitrary two-to-one functions after only $O(\sqrt[3]{N})$ expected evaluations of the function, where N is the cardinality of the domain. This should be compared with the best possible classical algorithm, which requires $O(\sqrt{N})$ expected evaluations when the function is provided as a black box. This has obvious consequences for the cryptanalysis of hash functions, unconditionally concealing bit commitment schemes and signature schemes based on claw-free pairs of functions.

More thorough, yet elementary, introductions to quantum computation can be found in [7, 1, 9, 5].

2 The Other Side of the Coin

The previous section is not precisely good news for those of us who simultaneously believe in quantum mechanics and in the legitimate need for protecting privacy. Fortunately, quantum mechanics may provide the ultimate solution to secure communication. Quantum cryptography exploits the impossibility to measure quantum information reliably. (Remember the wise words of Paul Simon: "The information's unavailable to the mortal man".) When information is encoded with non-orthogonal quantum states, any attempt from an eavesdropper to access it necessarily entails a probability of spoiling it irreversibly, which can be detected by the legitimate users. Using protocols designed in collaboration with Charles H. Bennett [4], building on earlier work of Stephen Wiesner [22], this phenomenon can be exploited to implement a key distribution system that is provably secure even against an eavesdropper with unlimited computing power, indeed even if the eavesdropper is equipped with a quantum computer. This is achieved by the exchange of very tenuous signals that consist on the average of one-tenth of one photon per pulse. Several exciting experimental realizations have been successful so far, demonstrating the feasibility of quantum key distribution over tens of kilometres of ordinary optical fibre or hundreds of meters in free space (no wave guides), and even the possibility of quantum cryptographic networks capable of linking many users. Whether or not quantum cryptography can go beyond key distribution and the secure transmission of confidential information is an actively researched topic.

Rather than repeating material that I have written too many times already, I invite you to read my *Sigact News* survey on 25 years of quantum cryptography [11].

3 And the Ugly?

Use your imagination!

Acknowledgements

I am very grateful to Burt Kaliski Jr and the entire CRYPTO 97 Programme Committee for inviting me to give this lecture. I also wish to acknowledge Charles H. Bennett, Claude Crépeau, Christopher Fuchs and William Wootters, who joined me on the occasion of the First Killam Workshop on Quantum Information Theory: our grilled octopus eating brainstorming session lead to the wonderful title of this talk. Chris provided the opening quote from *Slip Slidin' Away.*

References

1. Barenco, A., "Quantum physics and computers", *Contemporary Physics*, Vol. 38, 1996, pp. 357–389.
2. Benioff, P., "Quantum mechanical Hamiltonian models of Turing machines", *Journal of Statistical Physics*, Vol. 29, no. 3, 1982, pp. 515–546.
3. Bennett, C. H., E. Bernstein, G. Brassard and U. Vazirani, "Strengths and weaknesses of quantum computing", *SIAM Journal on Computing*, to appear, 1997.
4. Bennett, C. H., F. Bessette, G. Brassard, L. Salvail and J. Smolin, "Experimental quantum cryptography", *Journal of Cryptology*, Vol. 5, no. 1, 1992, pp. 3–28.
5. Berthiaume, A., "Quantum computation", in *Complexity Theory Retrospective II*, L. A. Hemaspaandra and A. Selman, editors, Springer-Verlag, Berlin, to appear, 1997.
6. Boyer, M., G. Brassard, P. Høyer and A. Tapp, "Tight bounds on quantum searching", *Proceedings of 4th Workshop on Physics and Computation*, Boston, November 1996, New England Complex Systems Institute, pp. 36–43. Available online in the *InterJournal* at URL `http://interjournal.org`. Improved version available from the authors.
7. Brassard, G., "A quantum jump in computer science", in *Computer Science Today*, Jan van Leeuwen (Editor), Lecture Notes in Computer Science, Vol. 1000, Springer–Verlag, 1995, pp. 1–14.
8. Brassard, G., "The impending demise of RSA?", *RSA Laboratories CryptoBytes*, Vol. 1, no. 1, 1995, pp. 1–4.
9. Brassard, G., "New trends in quantum computing", *Proceedings of 13th Annual Symposium on Theoretical Aspects of Computer Science*, February 1996, pp. 3–10.
10. Brassard, G., "Searching a quantum phone book", *Science*, Vol. 275, 31 January 1997, pp. 627–628.
11. Brassard, G. and C. Crépeau, "Cryptology column — 25 years of quantum cryptography", *Sigact News*, Vol. 27, no. 3, 1996, pp. 13–24.
12. Brassard, G., P. Høyer and A. Tapp, "Cryptology column — Quantum cryptanalysis of hash and claw-free functions", *Sigact News*, Vol. 28, no. 2, June 1997, pp. 14–19.
13. Deutsch, D., "Quantum theory, the Church–Turing principle and the universal quantum computer", *Proceedings of the Royal Society*, London, Vol. A400, 1985, pp. 97–117.
14. Diffie, W. and M. E. Hellman, "New directions in cryptography", *IEEE Transactions on Information Theory*, Vol. IT–22, no. 6, 1976, pp. 644–654.
15. Feynman, R. P., "Simulating physics with computers", *International Journal of Theoretical Physics*, Vol. 21, nos. 6/7, 1982, pp. 467–488.

16. Feynman, R. P., "Quantum mechanical computers", *Optics News*, February 1985. Reprinted in *Foundations of Physics*, Vol. 16, no. 6, 1986, pp. 507–531.
17. Grover, L. K., "A fast quantum mechanical algorithm for database search", *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, 1996, pp. 212–219. Final version to appear in *Physical Review Letters* under title "Quantum mechanics helps in searching for a needle in a haystack".
18. Haroche, S. and J.–M. Raimond, "Quantum computing: Dream or nightmare?", *Physics Today*, August 1996, pp. 51–52.
19. Los Alamos National Laboratory, "Quantum physics e-print archive": for the latest papers on the implementation of quantum computation and on quantum error correction, as well as just about everything of interest for quantum computing, quantum cryptography and quantum information theory in general, surf the Web from URL `http://xxx.lanl.gov/archive/quant-ph`.
20. Rivest, R. L., A. Shamir and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", *Communications of the ACM*, Vol. 21, no. 2, 1978, pp. 120–126.
21. Shor, P. W., "Algorithms for quantum computation: Discrete logarithms and factoring", *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science*, 1994, pp. 124–134. Final version to appear in *SIAM Journal on Computing* under title "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer".
22. Wiesner, S., "Conjugate coding", *Sigact News*, Vol. 15, no. 1, 1983, pp. 78–88; original manuscript written *circa* 1970.