AN UPDATE ON QUANTUM CRYPTOGRAPHY

Charles H. Bennett[1] & Gilles Brassard[2]

[1] IBM Research, Yorktown Heights, NY 10598
(Current address: Boston University
Computer Science Department, Boston, MA)

[2] Université de Montréal, Département IRO,
C.P. 6128, Succ. "A", Montréal (Québec), Canada H3C 3J7
(Current address: University of California,
Computer Science Division, 573 Evans Hall,
Berkeley, CA 94720)

INTRODUCTION

Although written about fifteen years ago, Wiesner's seminal paper, to which the origin of quantum cryptography must be traced back, did not appear in print until the spring of 1983 [W83]. The first published account of these ideas thus appeared in the proceedings of the second annual CRYPTO conference [BBBW83]. However, the concepts presented there were mostly of theoretical interest, because the technology involved in implementing them would have been far beyond the reach of our current knowledge. In particular, single polarized photons had to be trapped, bouncing back and forth between perfectly reflecting mirrors, and perfect efficiency in photon detection was required. To make up for this inconvenience, we could prove that no technology whatsoever, as well as no amount of computing power, could break some of our schemes, as long as some of the most fundamental principles of quantum physics hold true.

During the two years that have elapsed since, quantum cryptography has come a long way towards practicality. The most important breakthrough was quite an obvious observation: God did not create photons as a storage medium, but rather as a communications device. This paved the way to a quantum channel on which passive eavesdropping is meaningless, whereas any significant amount of active tampering has a high probability of being detected. The purpose of this Update is to present a short summary of the new results, and to stress how they differ from the current trend in cryptography.

G.R. Blakley and D. Chaum (Eds.): Advances in Cryptology - CRYPTO '84, LNCS 196, pp. 475-480, 1985.
© Springer-Verlag Berlin Heidelberg 1985

THE CURRENT TREND IN CRYPTOGRAPHY

Conventional cryptosystems, such as Enigma [G79], DES [NBS77] and even RSA [RSA78] are based on a mixture of mathematics, guesswork and wishful thinking. Shannon's information theory [Shan48, Shan49] does not take into account the amount of computing power at the enemy's disposal. On the other hand, the theory of computational complexity is not yet well enough understood to prove the computational security of public-key cryptosystems [DH76]. Even the theory of NP-completeness [GJ79] is unlikely to bear any relevance to cryptography [Br79].

The need for such proofs was dramatically emphasized when Shamir [Sham82, BS83] first explained at CRYPTO 82 how to break the basic Merkle-Hellman knapsack scheme [MH78]. Unfortunately, until the P=?NP question is settled [GJ79], the security of any public-key cryptosystem is doomed to depend on experience and unproved conjectures. The following quote from the original paper on (now broken) knapsack schemes is quite eloquent: "Faith in the security of these systems must therefore rest on intuition and on the failure of concerted attempts to break them" [MH78]. This is so reminiscent of what used to be said about World War II and earlier ciphers that one can only shiver at the thought that such is still the current situation. The following quotes, from an excellent tutorial introduction to cryptography by Diffie and Hellman, are certainly not obsolete, although some progress has been achieved in the past five years: "Cryptography is currently an engineering subject in which there are more facts and rules of thumb than theorems or systematic developments", and "We expect that provably secure systems will be developed as computer science progresses, but until that time, the current process of certification by mock attack will remain the most reliable test of a system's strength" [DH79].

Even the truly remarkable notion of probabilistic encryption, as set forth by Goldwasser and Micali in recent years [GM84], is not immune to an eventual breakthrough in algorithm design. The superb mathematics underlying these schemes can only serve to weaken the assumptions needed to infer their security. Nonetheless, they are also ultimately based on unproved conjectures in computational number theory. They have only changed the process of certification, which can concentrate on finding efficient algorithms for the relevant number theory problems, instead of working directly on pieces of ciphertext. Perhaps even more disturbing is the thought that such efficient algorithms may very well have been discovered already, but that they are being kept secret for obvious intelligence reasons, or in the hope of reaping a substantial profit.

It is nonetheless possible to prove *negative* theorems about mathematically based cryptosystems. For instance, Shannon proved that no traditional secret-key cryptosystem can achieve perfect secrecy against unlimited computing power, unless the key, used once only, is at least as long as the cleartext. Similarly, it is not hard to prove that any public-key distribution scheme [DH76] can be broken, given sufficient computing power, even if the cryptanalyst is only allowed passive eavesdropping.

QUANTUM CRYPTOGRAPHY

The purpose of quantum cryptography is to propose a radically different foundation for cryptography, viz. the uncertainty principle of quantum physics [Bo51]. Quantum cryptography can achieve most of the benefits of public-key cryptography, with the additional advantage of being provably secure, even against an opponent with superior technology and unlimited computing power, barring fundamental violations of accepted physical laws. It can be roundly asserted that any successful attack on some of our schemes would have more far reaching consequences on contemporary physics than an efficient factoring algorithm, or even a proof that P=NP (sic), would have on mathematics and computer science. Perhaps even more remarkable is the fact that quantum cryptography allows for protocols that achieve both mathematically impossible feats discussed at the end of the previous section.

Offsetting these advantages is the practical disadvantage that quantum transmissions are necessarily very weak and cannot be amplified in transit. However, a recent experiment conducted in France by Aspect, Grangier and Roger [AGR82] in order to test the Einstein-Podolsky-Rosen-Bohm gedankenexperiment [EPR35, M81] clearly indicated that quantum cryptography is within the reach of current technology, although more work is necessary for it to become economical and practical. Another disadvantage of quantum cryptography is that it does not provide digital signature [DH76] and related features, such as certified mail [Bl83a] or the ability to settle a dispute before the judge. However, these limitations seem to be inherent to any scheme secure against unlimited computing power. Also, the proposed coin tossing scheme discussed below is not secure against very advanced technology.

Readers interested in implementation details of the various quantum cryptography schemes are refered to other conference proceedings [BBBW83, BB83, BB84]. Let us only briefly describe here the basic underlying principles. In conventional information theory and cryptography, it is taken for granted that digital communications can always be monitored and copied, even by someone ignorant of their meaning. Such copies can be stored for an eventual future use, such as helping the decryption of later transmissions enciphered with the same secret key. However, when elementary quantum systems, such as polarized photons, are used to transmit digital information, the uncertainty principle gives rise to novel cryptographic phenomena, unachievable with traditional transmission media. This principle can be used effectively to design a communications channel whose transmissions in principle cannot be read or copied reliably by an eavesdropper ignorant of certain key information used in forming the transmission. The eavesdropper cannot even gain partial information about such a transmission without altering it in a random and uncontrollable way, likely to be detected by the channel's legitimate users.

Such a channel allows the unlimited re-use of a one-time pad without any breach of security, thus contradicting a well-established theorem of Shannon's. Whenever eavesdropping occurs, the enemy can gain no information on the message that was being sent, but the channel's legitimate users are warned that eavesdropping was attempted. A new secret key must then be used to retransmit the previous message, as well as for all further transmissions. As this new key could have been sent through the quantum channel as a previous secure transmission using an older key, this scheme has been described as a self-winding one-time pad.

More interestingly, the quantum channel achieves one of the main advantages of public-key cryptography by permitting secure distribution of random key information between two parties who share no secret information initially, provided both parties have access, beside the quantum channel, to an ordinary channel susceptible to passive eavesdropping, but not to active tampering. Even in the presence of active tampering, the two parties can still distribute a key securely if they share some much shorter secret information initially, provided the tampering is not so frequent as to suppress communications completely. These key distribution and key expansion schemes remain secure even if the enemy has unlimited computing power. Recall that it is a theorem that this is impossible to achieve for mathematically based schemes.

Finally, we also have a protocol for coin tossing [B183b] by exchange of quantum messages, which is secure against traditional kinds of cheating, even by an opponent with unlimited computing power. Ironically, it can be subverted by use of a still subtler quantum phenomenon, the already mentioned Einstein-Podolsky-Rosen-Bohm gedankenexperiment. This threat is merely theoretical, however, because it requires perfect efficiency of storage and detection of photons, which though not impossible in principle, is far beyond the capabilities of current technology. The honestly followed protocol, on the other hand, could be realized with current technology.

There is an interesting similarity between probabilistic encryption and quantum cryptography: both rely on the notion of reduction. However, whereas the former reduces the unproved computational complexity of some outstanding problems of number theory to the difficulty of breaking the schemes, the latter relies on the most fundamental beliefs of quantum physics. For instance, one such reduction can be used to prove about one of the coin tossing opponents that any systematic advantage he could get on the outcome of the coin toss could be used to effectively transmit information faster than the speed of light.

REFERENCES

[AGR82] Aspect, A., P. Grangier and G. Roger, "Experimental Realization of the Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: a New Violation of Bell's Inequalities", *Physical Review Letters*, Vol. 49, pp. 91-94 (1982).

[BB83] Bennett, C. H. and G. Brassard, "Quantum Cryptography, and its Application to Provably Secure Key Expansion, Public-Key Distribution, and Coin Tossing", *IEEE International Symposium on Information Theory*, St-Jovite, Quebec (1983).

[BB84] Bennett, C. H. and G. Brassard, "Quantum Cryptography: Public-Key Distribution and Coin Tossing", *Proceedings of the International Conference on Computers, Systems and Signal Processing*, Bangalore, India (1984).

[BBBW83] Bennett, C. H., G. Brassard, S. Breidbart and S. Wiesner, "Quantum Cryptography, or Unforgeable Subway Tokens", *Advances in Cryptography: Proceedings of CRYPTO 82*, Plenum Press, pp. 267-275 (1983).

[B183a] Blum, M., "How to Exchange (Secret) Keys", *ACM Transactions on Computer Systems*, Vol. 1, no 2, pp. 175-193 (1983).

[B183b] Blum, M., "Coin Flipping by Telephone - A Protocol for Solving Impossible Problems", *SIGACT NEWS*, Vol.15, no 1, pp. 23-27 (1983).

[Bo51] Bohm, D., *Quantum Theory*, Prentice Hall, Englewood Cliffs, NJ (1951).

[Br79] Brassard, G., "A Note on the Complexity of Cryptography", *IEEE Transactions on Information Theory*, Vol. IT-25, no 2, pp. 232-233 (1979).

[BS83] Brickell, E. F. and G. J. Simmons, "A Status Report on Knapsack Based Public Key Cryptosystems", *Congressum Numerantium*, Vol. 37, pp. 3-72 (1983).

[DH76] Diffie, W. and M. E. Hellman, "New Directions in Cryptography", *IEEE Transactions on Information Theory*, Vol. IT-22, pp. 644-654 (1976).

[DH79] Diffie, W. and M. E. Hellman, "Privacy and Authentication: an Introduction to Cryptography", *Proceedings of the IEEE*, Vol. 27, no 3, pp. 397-427 (1979).

[EPR35] Einstein, A., B. Podolsky and N. Rosen, *Physical Review*, Vol. 47, p. 777 (1935).

[G79] Garlinski, J., *The Enigma War*, Charles Scribner's Sons, New York, NY (1979).

[GJ79] Garey, M. R. and D. S. Johnson, *Computers and Intractability, a Guide to NP-Completeness*, W. H. Freeman and Co., San Francisco, CA (1979).

[GM84] Goldwasser, S. and S. Micali, "Probabilistic Encryption", *Journal of Computer and System Sciences*, Vol. 28, pp. 270-299 (1984).

[M81] Mermin, N. D., "Bringing Home the Atomic World: Quantum Mysteries for Anybody", *American Journal of Physics*, Vol. 49, no 10, pp. 940-943 (1981).

[MH78] Merkle, R. C. and M. E. Hellman, "Hiding Information and Signatures in Trapdoor Knapsacks", *IEEE Transactions on Information Theory*, Vol. IT-24, no 5, pp. 525-530 (1978).

[NBS77] ---, "Data Encryption Standard", *National Bureau of Standards*, FIPS PUB 46, Washington, DC (1977).

[RSA78] Rivest, R. L., A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", *Communications of the ACM*, Vol. 21, no 2, pp. 120-126 (1978).

[Sham82] Shamir, A., "A Polynomial Time Algorithm for Breaking the Basic Merkle-Hellman Cryptosystem", *Proceedings of the 23rd Annual IEEE Symposium on the Foundations of Computer Science*, pp. 145-152 (1982).

[Shan48] Shannon, C. E., "A Mathematical Theory of Communication", *Bell System Technical Journal*, Vol. 27, pp. 379-423, 623-656 (1948).

[Shan49] Shannon, C. E., "Communication Theory of Secrecy Systems", *Bell System Technical Journal*, Vol. 28, pp. 656-715 (1949).

[W83] Wiesner, S., "Conjugate Coding", unpublished manuscript written ca 1970, subsequently made available in *SIGACT NEWS*, Vol. 15, no 1, pp. 78-88 (1983).