Cryptographic Primitives and Quantum Theory

Claude Crépeau

Laboratoire d'Informatique de l'École Normale Supérieure (CNRS URA 1327) *

Abstract

This paper summarizes the current knowledge in the field of two-party cryptographic protocols devised from quantum systems. We introduce the reader to the notion of cryptographic protocols and describe a number of simple building blocks to achieve them. We also give pointers for the reader who is interested to the quantum implementation of these building blocks.

1 Introduction

Since the 1970's the science of secret writing, cryptography, has changed substantially due to the introduction of "public key cryptosystems" [26, 41]. The many properties of certain instances of these systems have open the door to several new applications (consult [42, 25, 29, 44, 34, 28, 7, 30, 36, 32, 11, 19, 33] for instance, to mention just a few). The initial goal of cryptography, to provide secure communications, has evolved into a variety of tasks involving secret data.

The scenario in which such tasks take place involves two participants (say Alice and Bob) who wish to perform some computation involving data they want to keep secret from one another. We call the solutions to such tasks "cryptographic protocols". An implementation of such a protocol is *secure* if a participant acting maliciously in any possible way he wishes cannot obtain more information about the other party's secret than what is described in the task's specification.

This paper introduces the reader to a number of cryptographic *primitives* used as building blocks to construct secure cryptographic protocols. It also contains pointers to a wide literature demonstrating how such building blocks can be implemented securely, not only using public key cryptography, but using quantum mechanics as a support.

* Département de Mathématiques et d'Informatique,
École Normale Supérieure,
45 rue d'Ulm, 75230 Paris CEDEX 05, France.
e-mail: crepeau@dmi.ens.fr.

2 Cryptographic Primitives

We now introduce the main two basic primitives that have been widely considered as useful building blocks in the design of more elaborate cryptographic protocols:

Bit commitment: Alice can commit to the value of a bit b in such a way that Bob has no information about which bit it is, yet Alice can only open the commitment to show the original bit b and not the opposite $\neg b$.

Oblivious transfer: Alice can send a bit b to Bob in such a way that the bit is received with probability 50%. Neither party can influence the probability that the bit is received. Alice obtains no information as to whether the transfer was successful, while Bob finds out with certainty.

Each of these two tasks have been first introduced in public-key cryptographic models and several results apply to them independently of their implementation. We now expand a little bit about each of them, their significance, and their quantum implementations.

2.1 Bit commitment

This primitive can be implicitly traced back to very early public-key cryptography papers [40, 42]. It as been used for **coin tossing protocols** (Alice and Bob who do not trust each other want to toss a coin over a telephone line) [8, 9, 2], **zero-knowledge proofs** (Alice wants to prove the validity of a statement to Bob without revealing him anything else than the fact that the statement is true) [35, 36, 12, 11, 32, 16, 10, 38], and more or less every single cryptographic protocol involves bit commitments somewhere. It is a very fundamental primitive.

In terms of quantum implementation, an early protocol to achieve this task was given implicitly in [2]: Bennett and Brassard gave a coin tossing protocol using faint pulses of polarized light which implicitly used bit commitment. Unfortunately, as explained in the same paper, their scheme can be defeated using pairs of entangled photons such as those suggested by Einstein, Podolsky and Rosen [27].

A later scheme [13], did not suffer from this attack. This time the possible flaw is linked to the assumption that photons are read individually. Although it was left as an open question in that paper, recent work with Richard Jozsa, Gilles Brassard and my student Denis Langlois indicates that general Positive Operator Measurements (POMs) will not have any impact on the security of this protocol. A realistic protocol which takes into account the parameters of the real prototype of the apparatus build by Bennett, Bessette, Brassard, Salvail and Smolin [5] can be deduced by the techniques used in [4] and [6].

2.2 Oblivious Transfer

A protocol with a flavour similar to Oblivious Transfer, called *multiplexing channel* by Wiesner [43], was one of the early applications of quantum mechanics for cryptography. Wiesner invented this protocol in the early 1970's, long before the cryptographers even realized the significance of this work. The Oblivious Transfer as described earlier is due to Rabin [40]. It has been used in the design of several more complicated protocols [8, 9, 40]. More formally correct versions of this protocol were later given by Fischer, Micali, and Rackoff in [30] and by Berger, Peralta and Tedrick in [7]. Other similar protocols were in the meanwhile introduced: Even, Goldreich and Lempel's *one-out-of-two oblivious transfer* [29] (which is more or less a stronger formal version of Wiesner's multiplexing) and All-or-Nothing Disclosure of Secrets (a generalization of one-out-of-two oblivious transfer) of Brassard, Crépeau and Robert [15].

All these different tasks were shown equivalent: any one of them can be implemented securely starting with a secure protocol of any other one of them [14, 20, 24, 23, 21]. In particular, any of these protocols can be used to achieve the following very general task [44, 33, 17, 39, 22]

Secure two party computation: Consider a two-parameter polynomial-time computable function f. One party knows input x and the other party knows input y. The protocol allows both parties to compute $f(x, y)$ without disclosing any information to either party about the other party's secret input, except of course for what can be inferred from knowledge of one's secret input and of the final output.

A large number of protocols can be described as an instance of secure two party computation. An example of this is Yao's "millionaire problem" [44]: Alice and Bob want to figure out which one of them is the richest without disclosing the value of their fortune to one another. Another example is what Damgård calls "the dating problem" [17]: Alice and Bob want to decide whether they are compatible for a date without revealing to each other the criterions according to which they would select a partner (for obvious reasons sometimes); they should find out nothing about their mutual tastes except for the fact that they were not compatible in the case were the protocol answers in that direction. Also, the widely studied "mental poker" problem [42, 34, 31, 1, 45, 18, 19, 33]: Alice and Bob want to play a fair game of poker in a setting where they cannot meet and exchange physical cards.

More seriously, a simple identification system can be set up as a particular case of the secure two party computation with the function f taken to be the boolean predicate $x = y$. This would enable two parties to check that they know a common identification string without disclosing any extra information in the case were they did not agree.

In the quantum world, several papers have suggested possible implementations of primitives equivalent to Oblivious Transfer, starting with Wiesner's paper [43]. Indeed the first published quantum solution to this problem was [3] (although Wiesner's original idea was conceived at least ten years before). Neither of these two protocols satisfied very strong security criteria. Recent work of Bennett and myself indicates that trivial extensions of these protocols might fulfill the strong security definitions. The result of this research has been rather disappointing since at least in the case of [3] this approach was shown insecure, while in the case of [43] it is still not clear if the new approach leads to a secure protocol or not.

More recently, a theoretical implementation of the one-out-of-two Oblivious Transfer was proposed in [23], but was totally useless in a realistic scenario were errors could occur during the quantum transmission.

A more complete description of that work and more thorough proofs may be found in [21].

Finally, joint work of myself with Bennett and Brassard, together with my student Marie-Hélène Skubiszewska, has led to a practical solution as explained in [6]. At this stage, the solution we have described has been experimentally exploited with the quantum prototype of [5]. Unfortunately, the error rate of the current apparatus is too high for the capabilities of our protocol. A new experiment is being set up with more accurate photodetectors.

3 Research Avenues

The main line of research that is currently being investigated concerning this work is the determination of the power of POMs as attacking tools against these systems. As mentioned above, work of Jozsa, myself, Brassard and Langlois (based on the wonderful book of Carl W. Helstrom [37]) seems to indicate that the protocols of [23, 13, 6] are safe even when Alice and Bob are allowed to attack them with POMs, but there is still a long way to go before absolute security of our solutions is proved.

Another line of research we are currently investigating is the possibility of implementing directly high level protocols such as the "x=y" primitive using quantum properties. Until now, it has been necessary to rely on several levels of *reductions* to transform the quantum transfer into something useful. This process is extremely costly and impractical.

Acknowledgments

I would like to thank all my collaborators for the work on this topic: Charles H. Bennett, Gilles Brassard, Richard Jozsa, Joe Kilian, Denis Langlois, Silvio Micali, Miklós Sántha, and Marie-Hélène Skubiszewska.

References

[1] I. Bárány and Z. Füredi. Mental poker with three or more players. *Information and Control*, 59:84–93, 1983.

[2] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, pages 175–179. IEEE, 1984.

[3] C. H. Bennett, G. Brassard, S. Breidbard, and S. Wiesner. Quantum cryptography. In *Proceedings CRYPTO 82*, pages 267–275. Plenum Press, 1983.

[4] C. H. Bennett, G. Brassard, and J.–M. Robert. Privacy amplification by public discussion. *SIAM J. Computing*, 17(2):210–229, April 1988.

[5] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. Experimental quantum cryptography. *Journal of Cryptology*, 5:3–28, 1992.

[6] C.H. Bennett, G. Brassard, C. Crépeau, and M.-H. Skubiszewska. Practical quantum oblivious transfer protocols. In *Advances in Cryptology: Proceedings of Crypto '91*, volume 576 of *Lecture Notes in Computer Science*, pages 351–366. Springer-Verlag, 1992.

[7] R. Berger, R. Peralta, and T. Tedrick. A provably secure oblivious transfer protocol. In T. Beth, N. Cot, and I. Ingemarsson, editors, *Proceedings of EUROCRYPT 84*, pages 379–386. Springer, 1985.

[8] M. Blum. Three applications of the oblivious transfer: Part i: Coin flipping by telephone; part ii: How to exchange secrets; part iii: How to send certified electronic mail. Technical report, Department of EECS, University of California, Berkeley, CA, 1981.

[9] M. Blum. Coin flipping by telephone. In *Proc. IEEE Spring COMPCOM*, pages 133–137. IEEE, 1982.

[10] G. Brassard, D. Chaum, and C. Crépeau. Minimum disclosure proofs of knowledge. *JCSS*, 37:156–189, 1988.

[11] G. Brassard and C. Crépeau. Non-transitive transfer of confidence: A perfect zero-knowledge interactive protocol for SAT and beyond. In 27^{th} *Symp. of Found. of Computer Sci.*, pages 188–195. IEEE, 1986.

[12] G. Brassard and C. Crépeau. Zero-knowledge simulation of boolean circuits (extended abstract). In A. M. Odlyzko, editor, *Advances in*

Cryptology: Proceedings of Crypto '86, volume 263 of *Lecture Notes in Computer Science*, pages 223–233. Springer-Verlag, 1987.

[13] G. Brassard and C. Crépeau. Quantum bit commitment and coin tossing protocols. In *Advances in Cryptology: Proceedings of Crypto '90*, volume 537 of *Lecture Notes in Computer Science*, pages 49–61. Springer-Verlag, 1991.

[14] G. Brassard, C. Crépeau, and J.–M. Robert. Information theoretic reductions among disclosure problems. In 27^{th} *Symp. of Found. of Computer Sci.*, pages 168–173. IEEE, 1986.

[15] G. Brassard, C. Crépeau, and J.–M. Robert. All-or-nothing disclosure of secrets (extended abstract). In A. M. Odlyzko, editor, *Advances in Cryptology: Proceedings of Crypto '86*, volume 263 of *Lecture Notes in Computer Science*, pages 234–238. Springer-Verlag, 1987.

[16] D. Chaum. Demonstrating that a public predicate can be satisfied without revealing any information about how. In A. M. Odlyzko, editor, *Proceedings CRYPTO 86*, pages 195–199. Springer, 1987. Lecture Notes in Computer Science No. 263.

[17] D. Chaum, I. Damgård, and J. van de Graaf. Multiparty computations ensuring privacy of each party's input and correctness of the result. In C. Pomerance, editor, *Advances in Cryptology: Proceedings of Crypto '87*, volume 293 of *Lecture Notes on Computer Science*, pages 87–119. Springer-Verlag, 1988.

[18] C. Crépeau. A secure poker protocol that minimizes the effects of player coalitions. In H. C. Williams, editor, *Advances in Cryptology: Proceedings of Crypto '85*, volume 218 of *Lecture Notes in Computer Science*, pages 73–86. Springer-Verlag, 1986.

[19] C. Crépeau. A zero-knowledge poker protocol that achieves confidentiality of the players' strategy or how to achieve an electronic poker face. In A. M. Odlyzko, editor, *Advances in Cryptology: Proceedings of Crypto '86*, volume 263 of *Lecture Notes in Computer Science*, pages 239–247. Springer-Verlag, 1987.

[20] C. Crépeau. Equivalence between two flavours of oblivious transfers (abstract). In C. Pomerance, editor, *Advances in Cryptology: Proceedings of Crypto '87*, volume 293 of *Lecture Notes in Computer Science*, pages 350–354. Springer-Verlag, 1988.

[21] C. Crépeau. *Correct and Private Reductions among Oblivious Transfers.* PhD thesis, Department of Elec. Eng. and Computer Science, Massachusetts Institute of Technology, 1990. Supervised by Silvio Micali.

[22] C. Crépeau. Verifiable disclosure of secrets and applications. In *Advances in Cryptology: Proceedings of Eurocrypt '89*, volume 434 of *Lecture Notes in Computer Science*, pages 181–191. Springer-Verlag, 1990.

[23] C. Crépeau and J. Kilian. Achieving oblivious transfer using weakened security assumptions. In 29^{th} *Symp. on Found. of Computer Sci.*, pages 42–52. IEEE, 1988.

[24] C. Crépeau and J. Kilian. Weakening security assumptions and oblivious transfer. In S. Goldwasser, editor, *Advances in Cryptology: Proceedings of Crypto '88*, volume 403 of *Lecture Notes in Computer Science*, pages 2–7. Springer-Verlag, 1990.

[25] R. A. DeMillo, N. Lynch, and M. J. Merritt. Cryptographic protocols. In *Proc. 14th ACM Symposium on Theory of Computing*, pages 383–400, San Francisco, 1982. ACM.

[26] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Trans. Inform. Theory*, IT-22:644–654, November 1976.

[27] A. Einstein, B. Podolsky, and N Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47:777, 1935.

[28] S. Even and O. Goldreich. On the security of multi-party ping-pong protocols. In *Proceedings of the 24th IEEE Symposium on Foundations of Computer Science*, pages 34–39, Tucson, 1983. IEEE.

[29] S. Even, O. Goldreich, and A. Lempel. A randomized protocol for signing contracts. In R. L. Rivest, A. Sherman, and D. Chaum, editors, *Proceedings CRYPTO 82*, pages 205–210, New York, 1983. Plenum Press.

[30] M. Fischer, S. Micali, and C. Rackoff. A secure protocol for the oblivious transfer, 1984. presented at EuroCrypt 84, the only manuscript

available is the extended abstract submitted to the conference.

[31] S. Fortune and M. Merrit. Poker protocols. In G. R. Blakley and D. C. Chaum, editors, *Advances in Cryptology: Proceedings of Crypto '84*, volume 196 of *Lecture Notes in Computer Science*, pages 454–464. Springer-Verlag, 1985.

[32] O. Goldreich, S. Micali, and A. Wigderson. Proofs that yield nothing but their validity and a methodology of cryptographic protocol design. In *Proceedings of the 27th IEEE Symposium on Foundations of Computer Science*, pages 174–187, Toronto, 1986. IEEE.

[33] O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game, or: A completeness theorem for protocols with honest majority. In *Proc. 19th ACM Symposium on Theory of Computing*, pages 218–229, New York City, 1987. ACM.

[34] S. Goldwasser and S. Micali. Probabilistic encryption and how to play mental poker keeping secret all partial information. In *Proc. 14th ACM Symposium on Theory of Computing*, pages 365–377, San Francisco, 1982. ACM.

[35] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof-systems. In *Proc. 17th ACM Symposium on Theory of Computing*, pages 291–304, Providence, 1985. ACM.

[36] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof-systems. *SIAM. J. Computing*, 18(1):186–208, February 1989.

[37] C.W. Helstrom. *Quantum Detection and Estimation Theory.* Academic Press, 1976.

[38] R Impagliazzo and M. Yung. Direct minimum-knowledge computations. In C. Pomerance, editor, *Advances in Cryptology: Proceedings of Crypto '87*, volume 293 of *Lecture Notes in Computer Science*, pages 40–51. Springer-Verlag, 1988.

[39] J. Kilian. Founding cryptography on oblivious transfer. In *Proc. 20th ACM Symposium on Theory of Computing*, pages 20–31, Chicago, 1988. ACM.

[40] M. Rabin. How to exchange secrets by oblivious transfer. Technical Report TR-81, Harvard Aiken Computation Laboratory, 1981.

[41] R. L. Rivest, A. Shamir, and L. M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communcations of the ACM*, 21:120–126, February 1978.

[42] A. Shamir, R. L. Rivest, and L. M. Adleman. Mental poker. In D. Klarner, editor, *The Mathematical Gardner*, pages 37–43. Wadsworth, Belmont, California, 1981.

[43] S. Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983. manuscript written *circa* 1970, unpublished until it appeared in SIGACT News.

[44] A. C. Yao. Protocols for secure computations. In *Proceedings of the 23rd IEEE Symposium on Foundations of Computer Science*, pages 160–164, Chicago, 1982. IEEE.

[45] M. Yung. Cryptoprotocols: Subscription to a public key, the secret blocking and the multi-player mental poker game. In G. R. Blakley and D. C. Chaum, editors, *Advances in Cryptology: Proceedings of Crypto '84*, volume 196 of *Lecture Notes in Computer Science*, pages 439–453. Springer-Verlag, 1985.