Cut-and-Choose protocols

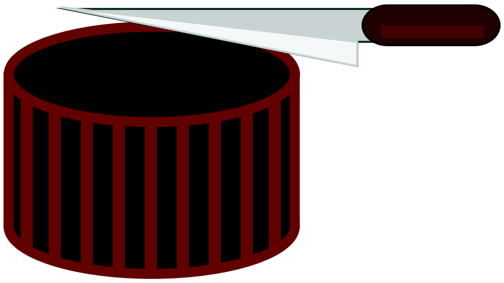
Claude Crépeau [*]

1 Cut-and-Choose protocol [C]

A cut-and-choose protocol is a two-party protocol in which one party tries to convince another party that some data he sent to the former was honestly constructed according to an agreed upon method. Important examples of cut-and-choose protocols are interactive proofs [GMR89], interactive arguments [BCC88], zero-knowledge protocols [GMR89, BCC88, GMW91], witness indistinguishable and witness hiding protocols [FS90] for proving knowledge of a piece of information that is computationally hard to find. Such a protocol usually carries a small probability that it is successful despite the fact that the desired property is not satisfied.

The very first instance of such a cut-and-choose protocol is found in the protocol of M. Rabin [Rab77] where the cut-and-choose concept is used to convince a party that the other party sent him an integer n product of two primes p, q each of which is congruent to 1 modulo 4. Note that this protocol was NOT zero-knowledge.

The expression cut-and-choose was later introduced by David Chaum [BCC88] in analogy to a popular cake sharing problem: Given a complete cake to be shared among two parties distrusting of each other (for reasons of serious appetite). A fair way for them to share the cake is to have one of them cut the cake in two equal shares, and let the other one choose his favourite share. This solution guarantees that it is in the formers best interest to cut the shares as evenly as possible.



References

[BCC88] G. Brassard, D. Chaum, and C. Crépeau. Minimum disclosure proofs of knowledge. *JCSS*, 37:156–189, 1988.

[FS90] U. Feige and A. Shamir. Witness indistinguishable and witness hiding protocols. In Baruch Awerbuch, editor, *Proceedings of the 22nd Annual ACM Symposium on the Theory of Computing*, pages 416–426, Baltimore, MY, May 1990. ACM Press.

[GMR89] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, 18(1):186–208, February 1989.

[GMW91] Oded Goldreich, Silvio Micali, and Avi Wigderson. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. *Journal of the Association for Computing Machinery*, 38(3):691–729, July 1991.

[Rab77] M. O. Rabin. Digitalized signatures. In Richard A. DeMillo et al., editors, *Foundations of Secure Computation: Papers presented at a 3 day workshop held at Georgia Institute of Technology, Atlanta, October 1977*, pages 155–166, New York, 1977. Academic Press.

[*] School of Computer Science, McGill University, Montréal (Qc), Canada H3A 2A7. e-mail: `crepeau@cs.mcgill.ca`.