# Everything in NP can be argued in *perfect* zero-knowledge in a *bounded* number of rounds

(Extended Abstract)

*Gilles BRASSARD* †
Département IRO
Université de Montréal

*Claude CRÉPEAU* ‡
Laboratory for Computer Science
Massachusetts Institute of Technology

*Moti YUNG*
IBM T. J. Watson Research Center
Yorktown Heights, NY

*ABSTRACT*

A perfect zero-knowledge interactive protocol allows a prover to convince a verifier of the validity of a statement in a way that does not give the verifier any additional information [GMR, GMW]. Such protocols take place by the exchange of messages back and forth between the prover and the verifier. An important measure of efficiency for these protocols is the number of rounds in the interaction. In previously known perfect zero-knowledge protocols for statements concerning **NP**-complete problems [BCC], at least $k$ rounds were necessary in order to prevent one party from having a probability of undetected cheating greater than $2^{-k}$. In the full version of this paper [BCY], we give the first perfect zero-knowledge protocol that offers arbitrarily high security for any statement in **NP** with a constant number of rounds (under a suitable cryptographic assumption). This protocol is a BCC-*argument* rather than a GMR-proof [BC3], as are all the known perfect zero-knowledge protocols for **NP**-complete problems [BCC].

† Supported in part by Canada NSERC grant A4107.
‡ Supported in part by an NSERC postgraduate scholarship; part of this research was performed while this author was visiting the IBM Almaden Research Center.

J.J. Quisquater and J. Vandewalle (Eds.): Advances in Cryptology - EUROCRYPT '89, LNCS 434, pp. 192-195, 1990.
© Springer-Verlag Berlin Heidelberg 1990

## History, motivation and main result

Much excitement was caused when it was discovered in 1986 by Goldreich, Micali and Wigderson that all statements in **NP** have *computational* zero-knowledge interactive proofs (under the assumption that secure encryption functions exist) [GMW]. See also [BC1]. Such proofs, a notion formalized by Goldwasser, Micali and Rackoff a few years previously, allow an infinitely powerful (but not trusted) prover to convince a probabilistic polynomial-time verifier of the validity of a statement in a way that does not convey any *polynomial-time-usable* knowledge to the verifier, other than the validity of the statement [GMR]. Informally, this means that the verifier should not be able to generate anything in probabilistic polynomial time after having participated in the protocol, that he could not have generated by himself without ever talking to the prover (from mere belief that the statement is true).

A result similar to those of [GMW, BC1] was obtained independently by Chaum, but under a very different model, which emphasizes the unconditional privacy of the prover's secret information, even if the verifier has unlimited computing power [Ch]. Independently, Brassard and Crépeau considered a model (compatible with Chaum's) in which all parties involved are assumed to have reasonable computing power, and they also obtained a protocol unconditionally secure for the prover (meaning that the prover's safety does not depend on unproved cryptographic assumptions) [BC2]. We shall refer to the settings of either [Ch] or [BC2] as the BCC-setting in order to contrast it with the GMR-setting described in the previous paragraph. Protocols in the BCC-setting are called *arguments* rather than proofs because even a polynomial-time prover could cheat them if the cryptographic assumption turns out to be false [BC3]. Joining forces, Brassard, Chaum and Crépeau subsequently showed that everything in **NP** can be argued in perfect zero-knowledge [BCC] (thanks to an idea of Damgaard), which implies that the prover's safety would still be guaranteed even if strong organizations with unknown computing power and algorithmic knowledge were to try to extract her secret and were willing to expend an arbitrary amount of time on this task.

The main motivation behind the work of [GMW, BC1, Ch, BC2, BCC] was a quest for *generality*: how much is it possible to prove in zero-knowledge if little attention is paid to efficiency? Other researchers were willing to sacrifice generality on the altar of efficiency. The best known instance of this approach is Feige, Fiat and Shamir's identification system [FFS], which handles an *ad hoc* problem relevant to the purpose of identification, but could not handle statements about **NP**-complete problems. One reason why the FFS scheme is so attractive in practice is that it requires only a few rounds of interaction between the prover and the verifier. In sharp contrast, the more general protocols of [GMW, BC1, Ch, BC2, BCC] require an unbounded number of rounds in order to achieve an arbitrarily high level of safety. This paper addresses the following question: Is it possible to combine generality and arbitrarily high safety with a small (constant?) number of rounds? (By one "round", we mean two "moves": one message sent by the verifier followed by one message sent by the prover.)

Our answer is that three rounds suffice under the assumption that it is possible to find a prime $p$ with known factorization of $p-1$ such that it is infeasible to compute discrete logarithms modulo $p$ even for someone who knows the factors of $p-1$, or more generally under the assumption that one-way group homomorphisms [IY] exist. Our three-round protocol and a sketch of the proof that it is perfect zero-knowledge can be found in the Proceedings of the 16th ICALP conference [BCY].

It should be pointed out that a similar question has been investigated independently by other researchers. In the GMR-setting, Goldreich and Kahn claim a bounded-round computational zero-knowledge protocol for all statements in **NP** [G]. Feige and Shamir have also developed a bounded-round computational zero-knowledge protocol for all statement in **NP**, but in a setting in which both the prover and the verifier are limited to probabilistic polynomial time [FS]. However, being merely *computational* zero-knowledge, neither of these protocols offer unconditional safety for the prover. Feige and Shamir also claim in [FS] that they have a bounded-round (in fact two rounds) *perfect* zero-knowledge protocol, but they give no detail in the currently available version of their paper (March 1989). Our ICALP paper [BCY] provides the first published bounded-round perfect zero-knowledge protocol for all statements in **NP** (in the BCC-setting).

**ACKNOWLEDGEMENTS**

It is a pleasure to acknowledge fruitful discussions with Charles H. Bennett, Joan Boyar, David Chaum, Ivan Damgaard, Uri Feige, Oded Goldreich, Joe Kilian, Phillip Rogaway and Adi Shamir.

**BIBLIOGRAPHY**

[BCC] Brassard, G., Chaum, D. and Crépeau, C., "Minimum disclosure proofs of knowledge", *Journal of Computer and System Sciences*, vol. 37, no. 2, 1988, pp. 156–189.

[BC1] Brassard, G. and Crépeau, C., "Zero-knowledge simulation of Boolean circuits", *Advances in Cryptology – CRYPTO '86 Proceedings*, Springer-Verlag, 1987, pp. 224–233.

[BC2] Brassard, G. and Crépeau, C., "Non-transitive transfer of confidence: A *perfect* zero-knowledge interactive protocol for SAT and beyond", *Proceedings of the 27th IEEE Symposium on Foundations of Computer Science*, 1986, pp. 188–195.

[BC3] Brassard, G. and Crépeau, C., "Sorting out zero-knowledge", *Advances in Cryptology – EUROCRYPT '89 Proceedings*, Springer-Verlag, to appear in this volume.

[BCY] Brassard, G., Crépeau, C. and Yung, M., "Everything in **NP** can be argued in *perfect* zero-knowledge in a *bounded* number of rounds", *Proceedings of 16th ICALP Conference*, Stresa, Italy, July 1989, to appear.

[Ch] Chaum, D., "Demonstrating that a public predicate can be satisfied without revealing any information about how", *Advances in Cryptology – CRYPTO '86 Proceedings*, Springer-Verlag, 1987, pp.195–199.

[FFS] Feige, U., Fiat, A. and Shamir, A., "Zero knowledge proofs of identity", *Journal of Cryptology*, vol.1, no.2, 1988, pp.77–94.

[FS] Feige, U. and Shamir, A., "Zero knowledge proofs of knowledge in two rounds", *Advances in Cryptology – CRYPTO '89 Proceedings*, Springer-Verlag, to appear.

[G] Goldreich, O., personal communication.

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

[GMR] Goldwasser, S., Micali, S. and Rackoff, C., "The knowledge complexity of interactive proof systems", *SIAM Journal on Computing*, vol.18, no.1, 1989, pp.186–208.

[IY] Impagliazzo, R. and Yung, M., "Direct minimum-knowledge computations", *Advances in Cryptology – CRYPTO '87 Proceedings*, Springer-Verlag, 1988, pp.40–51.