

Honest Verifier vs Dishonest Verifier in Public Coin Zero-Knowledge Proofs

Ivan Damgård* Oded Goldreich[†] Tatsuaki Okamoto[‡]
Avi Wigderson[§]

September 12, 1995

Abstract

This paper presents two transformations of public-coin/Arthur-Merlin proof systems which are zero-knowledge *with respect to the honest verifier* into (public-coin/Arthur-Merlin) proof systems which are zero-knowledge *with respect to any verifier*.

The first transformation applies only to constant-round proof systems. It builds on Damgård's transformation (see *Crypto93*), using ordinary hashing functions instead of the interactive hashing protocol (of Naor, Ostrovsky, Venkatesan and Yung – see *Crypto92*) which was used by Damgård. Consequently, the protocols resulting from our transformation have much lower round-complexity than those derived by Damgård's transformation. As in Damgård's transformation, our transformation preserves statistical/perfect zero-knowledge and does not rely on any computational assumptions. However, unlike Damgård's transformation, the new transformation is not applicable to argument systems or to proofs of knowledge.

The second transformation can be applied to proof systems of arbitrary number of rounds, but it only preserves statistical zero-knowledge. It assumes the existence of secure commitment schemes and transforms any public-coin proof which is statistical zero-knowledge with respect to the honest into one which is statistical zero-knowledge (in general). It follows, by a result of Ostrovsky and Wigderson (1993), that any language which is "hard on the average" and has a public-coin proof system which is statistical zero-knowledge with respect to the honest verifier, has a proof system which is statistical zero-knowledge (with respect to any verifier).

*Dept. of Computer Science, Aarhus University, Denmark and BRICS, Basic Research In Computer Science, center of the Danish National Research Foundation.

[†]Dept. of Computer Science and Applied Math., Weizmann Institute of Science, Rehovot, Israel. Work done while visiting BRICS, Basic Research In Computer Science, center of the Danish National Research Foundation. Supported in part by grant No. 92-00226 from the United States – Israel Binational Research Foundation (BSF), Jerusalem, Israel.

[‡]NTT Laboratories, Yokosuka-shi, 238-03 Japan. Work done while visiting AT&T Bell Laboratories, Murray Hill, NJ, USA

[§]Institute for Computer Science, Hebrew University, Jerusalem, Israel. Work done while visiting BRICS, Basic Research In Computer Science, center of the Danish National Research Foundation. This research was partially supported by a grant from the Wolfson Research Awards, administered by the Israeli Academy of Sciences and Humanities.