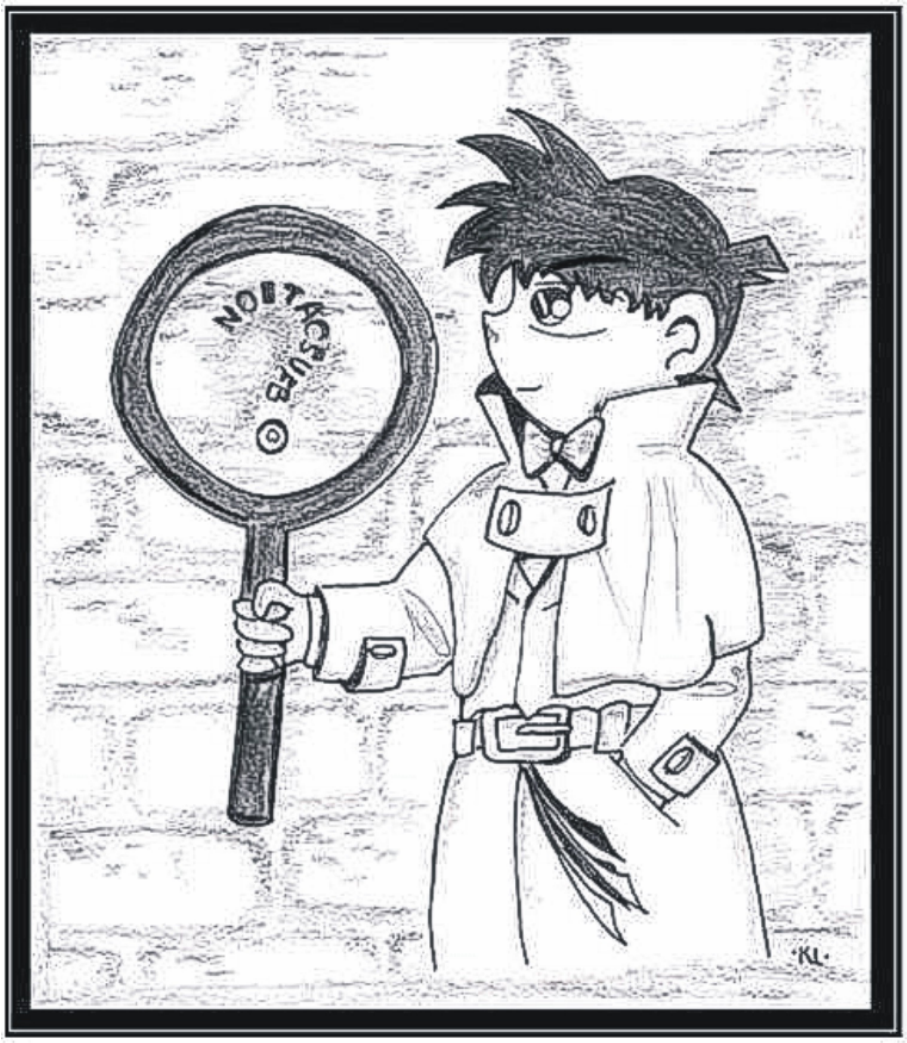
- The 2006 MILNER LECTURE -

On the Impossibility of Obfuscation

Shafi Goldwasser

MIT



5.15pm Wednesday, 7 June 2006
Swann Lecture Theatre, Swann Building, King's Buildings, Edinburgh

Informally, program obfuscation aims at making a program "unintelligible" while preserving its functionality. Whereas practitioners have been engaged in attempts of program obfuscation for many years for purposes of defeating software reverse engineering, its mere theoretical possibility has only recently received attention in the theoretical community. Results on the topic point in two directions; on the one hand, there is a formal model of obfuscation in which there are provably non-obfuscatable functions; on the other, it was shown that at least one entire class of (rather simple) functions can be obfuscated. Thus, it seemed completely possible that most functions of interest can be obfuscated even though in principle general purpose obfuscators do not exist. In this talk we will show that this is unlikely to be the case. We first argue that any *useful* positive result about the possibility of obfuscation must also cover the case where the adversary has certain auxiliary information. We will then prove that there exist many *natural* classes of functions that cannot be obfuscated w.r.t. auxiliary input, both when the input is dependent on the function being obfuscated and even when it is *independent* of the function being obfuscated.

School of informatics

The Milner Lecture is a public lecture, open to all, hosted by the Laboratory for Foundations of Computer Science of The University of Edinburgh. The Milner Lecture provides a distinguished forum for excellence and original theoretical work which has a perceived significance for practical computing.