1011-68-355 **Dan Gutfreund** (danig@cs.huji.ac.il), The Hebrew University, Jerusalem, Israel, **Ronen Shaltiel** (ronen@cs.haifa.ac.il), University of Haifa, Haifa, Israel, and **Amnon Ta-Shma*** (amnon@tau.ac.il), Tel-Aviv University, Tel-Aviv, Israel. *If NP languages are hard on the worst-case then it is easy to find their hard instances.*

We prove that if NP is not in BPP, i.e., if some NP-complete language is worst-case hard, then for every probabilistic algorithm trying to decide the language, there exists some polynomially samplable distribution that is hard for it. That is, the algorithm often errs on inputs from this distribution. This is the first worst-case to average-case reduction for NP of any kind.

We stress however, that this does not mean that there exists one fixed samplable distribution that is hard for all probabilistic polynomial time algorithms, which is a pre-requisite assumption needed for OWF and cryptography (even if not a sufficient assumption). Nevertheless, we do show that there is a fixed distribution on instances of NP-complete languages, that is samplable in quasi-polynomial time and is hard for all probabilistic polynomial time algorithms (unless NP is easy in the worst-case).

Our results are based on the following lemma that may be of independent interest: Given the description of an efficient (probabilistic) algorithm that fails to solve SAT in the worst-case, we can efficiently generate at most three Boolean formulae (of increasing lengths) such that the algorithm errs on at least one of them. (Received August 30, 2005)