Report on the thesis "Logic and cryptography", Vojtěch Wagner

Impagliazzo and Kapron in [IK03] present a formal logical system for reasoning about cryptography, with the aim of developing clean formal methods for proving that cryptographic constructions are secure. One of their sample proofs shows that the output of a pseudorandom generator can be "stretched" in a secure way. The goal of this thesis is to show that the Goldreich-Levin theorem is provable in their system. This theorem states that from a one-way function we can construct another one-way function which has a hard bit, and is a major ingredient in constructing pseudorandom generators (and has other applications).

This result would be interesting to know, and is unlikely to require any new ideas. However the proof given in the thesis does not work. The biggest issue is that arguments about probability need to be translated carefully into statements about counting basic formulas, and then proved by appealing to the counting axioms provided by the system. The candidate fails to do either of these. The result is that the thesis, although it deals just about adequately with surface issues, does not address the real problem. There are also many smaller mistakes, inconsistent or careless uses of notation, misunderstandings, and confusing comments that seem to come from nowhere.

For example: Definition 3.6 does not make much sense, since expectation and variance are defined for random variables, not for formulas, and because large sums cannot be defined using LRN. In Lemma 3.4 the notation for probability is incoherent (since we are not considering probabilities over x) and changes twice during the proof. In the actual application, the main technical Lemma 3.5, the random variable is a sum of Boolean values. What is needed is a careful formalization of this as a counting term, and a version of the Chebyshev inequality for this particular kind of formalization.

The candidate has clearly studied the background material, is capable of writing mathematics and laying out a thesis in a reasonable way, and understands the algorithms and cryptography side fairly well. The initial presentation of the logical system is not too bad, and the formalization of the statement of Goldreich-Levin is done neatly, as are some of the algorithms.

Neil Thapen 31 August 2015