Public Key Cryptography from Different Assumptions

Benny Applebaum* Boaz Barak† Avi Wigderson‡

December 31, 2008

Abstract

This paper attempts to broaden the foundations of public-key cryptography. We construct a new public key encryption based on two "hardness on average" assumptions: **(1)** it is hard to "learn parity with noise" for random sparse equations, and **(2)** it is hard to approximate the vertex expansion of random unbalanced bipartite graphs.

More precisely, we show that a semantically secure public-key encryption scheme is implied by the following:

For some $m > n > d$ and q, μ satisfying $\mu \ll 1/q$

1. It is hard to distinguish between **(a)** a random set of m equations on n variables in GF(2) such that each equation involves d variables, and **(b)** a random set of such equations that have a solution satisfying $1 - \mu$ fraction of them.
2. It is hard to distinguish between **(a)** a random bipartite graph whose left and right sides have m and n vertices respectively and whose left degree is d, and **(b)** a random such graph that has a subset of q left vertices with at most $q - 1$ neighbors.

We also construct a public-key encryption scheme based on a variant of Assumption 1 with *non-linear* equations (and no noise) as long as Assumption 2 holds for $q = O(\log n)$.

Most, if not all, previous constructions of public key encryption used hardness assumptions with significant algebraic structure. Our new assumptions, positing indistinguishability from uniform of certain natural distributions on instances of **NP**-complete problems, seem relatively unstructured and qualitatively different from previous ones.

We give some evidence for these assumptions by studying their resistance to certain natural algorithms, and relating them to variants of more widely studied assumptions such as the hardness of the "search version" of learning parity with noise and the planted clique problems.

Keywords: Public key encryption, expander graphs, cryptography in NC0, lossless expanders, unbalanced expanders, planted problems

[*] Department of Computer Science, Princeton University, benny.applebaum@gmail.com . Supported by NSF grants CNS-0627526, CCF-0426582 and CCF-0832797.

[†] Department of Computer Science, Princeton University, boaz@cs.princeton.edu. Supported by NSF grants CNS-0627526, CCF-0426582 and CCF-0832797, US-Israel BSF grant 2004288 and Packard and Sloan fellowships.

[‡] Institute for Advanced Study, Princeton, NJ, avi@ias.edu.