Отчёт за 2007 г. по гранту фонда «Династия»

Э.А.Гирш

1 Научная деятельность

Предположим, что существует функция f, вычислимая за полиномиальное время, обратная к которой не вычислима за вероятностное полиномиальное время в среднем. В отличие от постановки «в среднем», в криптографической постановке всякий возможный полиномиальный вероятностный противник должен ошибаться на полиномиальной доле входов. Тем не менее, мы показываем, как модифицировать функцию f так, чтобы получить функцию, одностороннюю в криптографическом смысле на бесконечной последовательности длин входов.

Эти результаты докладывались в Москве на Workshop on Computational, Descriptive and Proof Complexity, and Algorithms и опубликованы в

[1] E.A.Hirsch, D.M.Itsykson, *An infinitely-often one-way function based on an average-case assumption*, Electronic Colloquium on Computational Complexity, Report TR07-117.

Также закончены и приняты два обзора по верхним оценкам на время работы в наихудшем случае алгоритмов для задачи булевой выполнимости:

[2] E.A.Hirsch, *Exact Algorithms for General CNF SAT*, In: Encyclopedia of Algorithms. Springer. To appear in 2008.

[3] E.Dantsin, E.A.Hirsch, *Worst-Case Upper Bounds*, In: Handbook of Satisfiability. IOS Press. To appear in 2008.

2 Преподавательская деятельность

Под моим руководством А.А.Кожевников защитил в мае 2007 года кандидатскую диссертацию на тему *«Сложность пропозициональных систем доказательств, оперирующих неравенствами»*.

Также я продолжаю осуществлять руководство четырьмя аспирантами, читаю лекции по курсам «Анализ алгоритмов» и «Сложностная криптография» на мат-мехе СПбГУ, веду специализированные студенческие семинары.

3 Научные планы на будущее

В 2008 г. я планирую продолжать заниматься сложностной криптографией и смежными вопросами. В частности, я собираюсь продолжить начатую в [3] деятельность по наведению мостов между криптографической и традиционной теорией сложности. Также я планирую заниматься сложностью «ослабленных» (“feebly”) односторонних функций и функций с секретом и другими нижними оценками сложности функций.