Отчёт за 2008 г. по гранту фонда «Династия»

Э.А.Гирш

1 Научная деятельность

Не известно функций, вычислимых за полиномиальное время, про которые было бы доказано, что обратные к ним за полиномиальное время не вычислимы — ни в наихудшем случае (что означало бы $\mathrm{P} \neq \mathrm{NP}$), ни в криптографическом смысле (когда имеется в виду вычислимость обратной хотя бы на какой-нибудь полиномиальной доле входов). Более того, не известно функций, для которых отношение схемной сложности обращения к сложности вычисления больше двух (результат Хильтгена 1992 г.).

Построение семейств «функций с секретом», которые трудно обратимы в вышеприведённом смысле, но легко обратимы, если известна «секретная информация», — ещё более трудная задача, являющаяся обобщением предыдущей. Мы строим семейство «функций с секретом», для которых отношение схемной сложности обращения без секрета к сложности вычисления и обращения с секретом больше 25/22.

Эти результаты опубликованы в препринте

E.A.Hirsch, S.I.Nikolenko, *A feebly secure trapdoor function*, PDMI preprint 16/2008.

Также закончены и приняты к публикации статьи

Д.Ю.Григорьев, Э.А.Гирш, К.В.Первышев, *Иерархии по времени с неравномерной подсказкой для криптографического обращения функций*, Записки научных семинаров ПОМИ, 2008 (в печати).

E.A.Hirsch, A.Kojevnikov, A.S.Kulikov, S.I.Nikolenko, *Complexity of Semialgebraic Proofs with Restricted Degree of Falsity*, Journal on Satisfiability, Boolean Modeling and Computation, 2008 (to appear).

2 Преподавательская деятельность

Под моим руководством трое аспирантов закончили в 2008 г. подготовку диссертаций (должны защищаться в 2009 г.), я продолжаю руководить ещё двумя аспирантами и несколькими студентами, читаю лекции по курсам «Информатика», «Анализ алгоритмов» и «Сложность вычислений» на мат-мехе СПбГУ, веду специализированные студенческие семинары.