Вопросы по курсу «Вычислительная криптография и сложность в среднем»

CR 1. Односторонние в наихудшем случае функции.

CR 2. Сильные и слабые односторонние функции.

CR 3. Примеры предположительно односторонних функций. Односторонние функции с полиномиально доступным распределением на входах. Универсальная односторонняя функция.

CR 4. Трудный бит и его существование с помощью вероятностного декодирования списком кодов Адамара.

CR 5. Вероятностное декодирование списком кодов Адамара.

CR 6. Вычислительная неразличимость. Односторонняя функция из генератора псевдослучайных чисел. Односторонние перестановки, примеры. Конструкция $(n+1)$-генератора на основе перестановки.

CR 7. Конструкция $p(n)$-генератора.

CR 8. Семейство псевдослучайных функций.

CR 9. Одноразовый и многоразовые протоколы с секретным ключом.

CR 10. Протокол с открытым ключом. Семейства односторонних перестановок с секретом, примеры.

CR 11. Неинтерактивный протокол привязки к биту.

CR 12. Интерактивный протокол привязки к биту.

CR 13. Стратегии, разглашающие только $f(x)$. Разглашение при многократном применении стратегии. Интерактивные доказательства с нулевым разглашением. Протокол для изоморфизма графов.

CR 14. Протокол с нулевым разглашением для языка из NP.

CR 15. Одноразовый протокол электронной подписи одного бита. Одноразовый протокол электронной подписи фиксированного полиномиального числа битов.

CR 16. Одноразовый протокол электронной подписи произвольных сообщений полиномиальной дли- ны на основе СТОК.

CR 17. Построение СТОК через СТОЗ. Конструкция СТОЗ.

CR 18. Одноразовый протокол электронной подписи произвольных сообщений полиномиальной длины на основе универсального семейства односторонних хеш-функций.

CR 19. Многоразовый протокол электронной подписи.

CR 20. Распределенные задачи. Полиномиальность в среднем по Левину и Импальяццо.

CR 21. Пример распределения, для которого сложность в среднем и наихудшем случае эквивалентны.

CR 22. Доминирование распределений. Универсальное полиномиально моделируемое распределение. Сведения. Полная задача в $(\mathrm{NP}, \mathrm{PSamp})$.

CR 23. Обратимые полиномиально моделируемые распределения (PISamp). Вычислимые распределения, включение $\mathrm{PComp} \subseteq \mathrm{PISamp} \subseteq \mathrm{PSamp}$. Полнота задачи об ограниченной остановке в $(NP, PISamp)$.

CR 24. Классы $\mathrm{HeurBPP}, \mathrm{AvgBPP}$, задачи поиска. Сведение задач поиска к задачам распознавания.

CR 25. Вероятностные сведения для задач поиска. Замкнутость класса $\widetilde{\mathrm{HeurBPP}}$ относительно этих сведений.

CR 26. Вероятностное сведение $(\mathrm{NP}, \widetilde{\mathrm{PSamp}})$ к $(\widetilde{NP, U})$.

CR 27. Из существования полной задачи с равномерным распределением относительно детерминированных сведений следует, что NEXP = EXP.

CR 28. Односторонние функции и трудные задачи в $(\mathrm{NP}, \mathrm{U})$. Построение бесконечно часто односторонней функции на основе функции, которая трудно обращается в среднем.