Вопросы по курсу "Сложностная криптография и сложность в среднем"

CR1. Односторонние в наихудшем случае функции. Односторонние функции, соглашения о длинах входа.

CR2. Сильные и слабые односторонние функции.

CR3. Семейство односторонних функций. Универсальная односторонняя функция.

CR4. Трудный бит и его существование.

CR5. Вычислительная неразличимость и ее свойства. Односторонняя функция из генератора псевдослучайных чисел. Конструкция $(n+1)$-генератора.

CR6. Конструкция $p(n)$-генератора. Протокол с секретным ключом.

CR7. Неразличимость повторных распределений.

CR8. Семейство псевдослучайных функций.

CR9. Неинтерактивный протокол привязки к биту.

CR10. Интерактивный протокол привязки к биту.

CR11. Доказательства с совершенно нулевым разглашением, доказательства с вычислительно нулевым разглашением. Протокол для изоморфизма графов.

CR12. Нулевое разглашение с использованием дополнительной информации. Нулевое разглашения для класса NP (схема доказательства).

CR13. Семейства односторонних перестановок с секретом, примеры. Протокол с открытым ключом.

CR14. Одноразовый протокол электронной подписи одного бита. Одноразовый протокол электронной подписи фиксированного полиномиального числа битов.

CR15. Одноразовый протокол электронной подписи произвольных сообщений полиномиальной длины на основе СТОК.

CR16. Построение СТОК через СТОЗ. Конструкция СТОЗ.

CR17. Одноразовый протокол электронной подписи произвольных сообщений полиномиальной длины на основе универсального семейства односторонних функций.

CR18. Многоразовый протокол электронной подписи.

CR19. Распределенные задачи. Полиномиальность в среднем по Левину и Импальяццо.

CR20. Пример распределения, для которого сложность в среднем и наихудшем случае эквивалентны.

CR21. Доминирование распределений. Универсальное полиномиально моделируемое распределение. Сведения. Полная задача в $(NP, PSamp)$.

CR22. Обратимые полиномиально моделируемые распределения ($PISamp$). Вычислимые распределения, включение $PComp \subseteq PISamp \subseteq PSamp$. Полнота задачи об ограниченной остановке в $(NP, PISamp)$.

CR23. Классы $HeurBPP$, $AvgBPP$, задачи поиска. Универсальные семейства хеш-функций. Лемма Вэлиэнта-Вазирани для универсального семейства хэш-функций.

CR24. Сведение задач поиска к задачам распознавания.

CR25. Вероятностные сведения для задач поиска. Замкнутость класса $\widetilde{HeurBPP}$ относительно этих сведений

CR26. Вероятностное сведение $(NP, PSamp)$ к (NP, U).

CR27. Из существования полной задачи с равномерным распределением относительно детерминированных сведений следует, что $NEXP = EXP$.

CR28. Односторонние функции и трудные задачи в (NP, U).