Краткое изложение заявки

Работа, которой я собираюсь заняться – изучение свойств булевых функций большого количества переменных. Во-первых, мне интересно распределение максимально нелинейных функций по всему множеству функций от заданного количества переменных. Сейчас уже получено полностью распределение для функций от 3-х, 4-х и 5-ти переменных. В данных распределениях (если их отобразить в графическом или табличном виде) прослеживается некоторая регулярность. В первоначальных планах на основе данной статистики построить процедуру (алгоритм), которая бы позволяла находить максимально-нелинейные функции, не используя полного перебора. В настоящее время аналитического или алгоритмического решения данной задачи не существует. Затем данная процедура будет проверена на функциях от большего количества переменных.

Также интересным является распределение весов булевых функций (имеется в виду вес Хэмминга). Планируется получить как минимум распределение значений весов для функций от 3-х, 4-х и 5-ти переменных. И затем исследовать его на предмет соответствия с распределением значений нелинейности.

Третьей, более сложной, задачей является установление связи между нелинейностями 2-х функций f и g и нелинейностью их композиции.

Все три перечисленные задачи сложны, прежде всего, в вычислительном плане. Поэтому получать необходимую статистику планируется при помощи вычислений на кластере (как это уже сделано для вычисления значений нелинейности), а также исследовать способы ускорения определения значения нелинейности.

Решаемые задачи имеют значение для алгебры и криптографии:

1) В случае удачи, процедура поиска максимально-нелинейных булевых функций позволит представить все множество функций от фиксированного количества переменных в виде структуры, которую можно будет промасштабировать и применить к множеству функций от большего количества переменных.
2) До сих пор слабо исследован вопрос влияния композиции функций на значение нелинейности результирующей функции. Можно ли таким образом получать функции с высоким значением нелинейности? Нет ли опасности, наоборот, используя нелинейные преобразования на разных раундах шифрования, получить в итоге преобразование линейное или близкое к линейному?
3) Выбор узлов замен блочных шифров с наилучшими характеристиками нелинейности, позволяет построить криптосистему с высокой степенью стойкости к дифференциальному и линейному криптоанализам.
4) При аппаратной реализации кодирования или шифрования использование булевых функций с меньшими весами позволяет разрабатывать более быстрые и экономичные решения.