Запрос на внешние инновации

|  |  |  |
| --- | --- | --- |
|  | Организация, ХК | АО «Концерн Автоматика» |
|  | Наименование ЗВИ,Обобщенное краткое наименование задачи | Алгоритмические подходы к вскрытию схемы Диффи-Хеллмэна на эллиптических кривых с использованием спариваний.  |
|  | Описание ситуации: ЦЕЛЬ, НАДСИСТЕМА,Проблема верхнего уровня, для решения которой ставится настоящая задача *(может быть несколько уровней иерархии целей)* | В связи с появившейся в 2004 году новой техникой для атаки на схемы открытого распределения ключа (ОРК) с использованием спариваний необходимо минимизировать риски для стойкости таких схем.1. Параметры ГОСТ Р34.10 2018 позволяют применить технологию со спариваниями к вскрытию систем ОРК.
2. Теория эллиптических кривых – сложная и широкая отрасль алгебраической геометрии. С другой стороны, эллиптические кривые – наиболее удобный объект для построения криптопротоколов (легко вычислять, но трудно обращать вычисления). Для препятствования применению новой технологии со спариваниями предложено изменить параметры используемых кривых относительно ГОСТ. Однако для некоторых криптопротоколов эти параметры неприемлемы.
 |
|  | Постановка задачи, кто, что и над чем должен сделать(субъект–действие – объект) | Анализ стойкости протоколов на эллиптических кривых относительно спариваний  |
|  | Объект (устройства, система, техпроцесс) | Российский стандарт цифровой подписи ГОСТ Р 34.10-2018 |
|  | Его функция | Позволяет предвидеть атаки на действующие протоколы цифровой подписи и открытого распределения ключа |
|  | Значения ключевых характеристик, которые требуется достичьДля проблемной ситуации укажите какова ее первопричина и в чем состоит «неразрешимый конфликт (противоречие) в требованиях.Допускается ли компромисс (оптимизация) | Выбрать параметры безопасности, исключающие подходы, связанные с построением спариваний на рассматриваемых эллиптических кривых. |
|  | Уровень ключевых характеристик мирового лидера | Имеется алгоритм вычисления функции по ее дивизору специального вида, полиномиальный по порядку используемых точек |