**Все или ничего**

Решение проблемы называется раскрытием секретов “Все или ничего”. Суть его заключается в том, что, если Боб получил любую информацию о любом секрете Алисы, он теряет шанс узнать что-либо еще о других ее секретах. Если есть уверенность, что участники этого рынка не могут создавать коалиции, то можно использовать следующий простой протокол.

1. А ➔ B:{}, где , т. е. Алиса зашифровывает все секреты с помощью RSA и посылает их Бобу

2. B ➔ A:{}, где , т. е. Боб выбирает свой секрет , генерирует случайное число и посылает Алисе

3. A ➔ B:{}, где

4. B: Боб вычисляет

Если участники могут создавать коалиции, т.е. жульничать, Боб перед проходом 2 может доказать с нулевым разглашением, что он знает некоторое r, такое что , и хранить b в секрете, пока Алиса не передаст ему на проходе 3 значение .