36 Телефонный справочник

Задача. Трент поручил Бобу разработать интерактивный телефонный справочник. Боб написал программу, которая на запрос `имя` отвечает парой (`имя`, `номер_телефона`), сопровождаемой подписью Трента. Подпись доказывает, что абонент с определенным именем действительно имеет определенный номер телефона. К сожалению, Боб не учел, что справочник покрывает только часть имен. Помогите Бобу модернизировать программу так, чтобы она дополнительно возвращала доказательство отсутствия в справочнике абонента с определенным именем. Доказательство должно представлять собой структуру данных, подписанную Трентом. Трент опасается передавать Бобу личный ключ подписи, поэтому все доказательства должны быть созданы Трентом заранее, в момент формирования справочника.

Решение. Имена в справочнике отсортированы лексикографически. Трент подписывает не только пары (`имя`, `номер_телефона`), но и пары соседних имен. Доказательством того, что имя N отсутствует в справочнике являются подписанная Трентом пара имен (A, B), между которыми N должно находиться:

$$A < N < B.$$

Подобного рода доказательства используются в DNSSEC. □