

10/02/2013

Sublinear secure computation?

- All protocols thus far were circuit-based
 - any circuit for a non-trivial function has linear size
- Any secure computation protocol requires at least linear time
 - if a party does not touch every bit of input, this leaks information

Idea:

- Move to a setting where parties evaluate some function l times
- Hope for complexity $O(n) + o(nl)$
 - \Rightarrow amortized complexity $O(n/l) + o(n)$
 - $\Rightarrow l$ large \Rightarrow sublinear amortized complexity
- Or preprocessing (expensive)
 - online computation sublinear in n

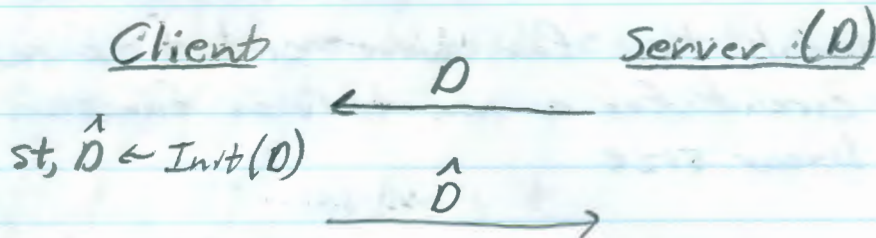
Example:

Binary-Search:

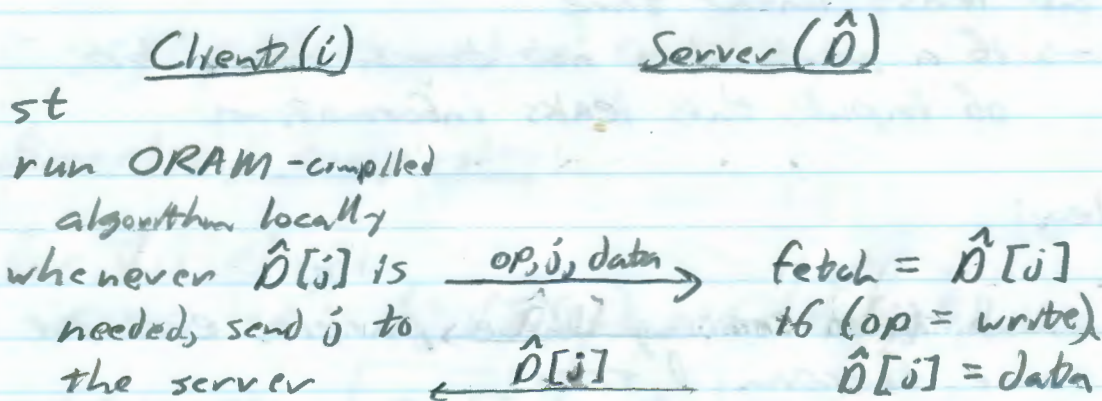
- Init setup
- For each binary-search computation
 - each lookup for the binary-search algorithm is compiled into a sequence of actual lookups in the ORAM.

One-sided secure protocol: (privacy of client)

initialization

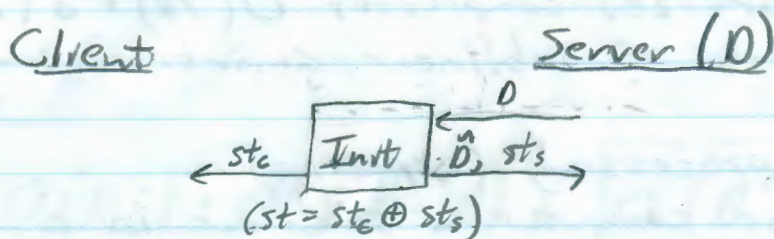


operations

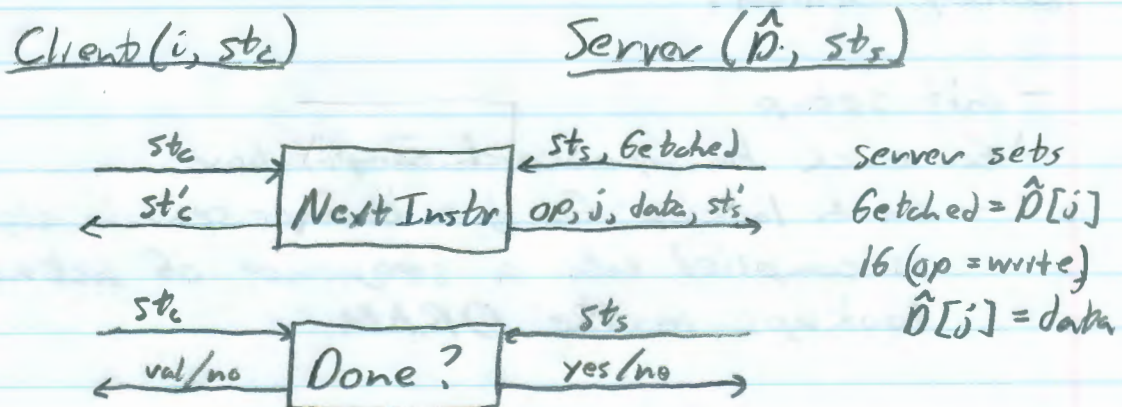


Two-sided secure protocol:

initialization



operations



Improvement: run for fixed # of steps

* Online: sublinear time
* Secure for semi-honest model

Generic Protocol:

- protocol that can securely evaluate any function in some specified class of functions
→ e.g. finite automaton

Special-purpose / tailored protocol:

- designed specifically for some function f

Problem:

Set Intersection:

each P_i has a set $S_i \subseteq \{0, 1\}^l$

Parties want to compute $S_1 \cap S_2$

ENP '04:

- homomorphic encryption-based solution

Observation:

$$\text{Let } P(x) = \sum_i a_i x^i$$

Given $[a_0], [a_1], \dots, [a_l], \gamma$

Can compute $[P(\gamma)]$

observation:

$$P_1(\{x_1, \dots, x_n\})$$

$$P_2(\{y_1, \dots, y_n\})$$

Encode its set as 0's
of a polynomial Q .

$$\text{i.e. } Q(x) = \prod_i (x - x_i)$$

$$Q(x) = \sum_i a_i \cdot x^i$$

$$\text{pk}, [a_0], [a_1], \dots, [a_n] \rightarrow$$

$$\text{compute } [Q(y_1)], \dots, [Q(y_n)]$$

$$\Downarrow$$
$$\text{compute } [r_i \cdot Q(y_i) + y_i]$$

$$[r_i \cdot Q(y_n) + y_n]$$

$$\leftarrow [r_i \cdot Q(y) + y], \dots, [r_i \cdot Q(y_n) + y_n]$$

decrypt...