### **Circuit ORAM**

Xiao Shaun Wang (UMD), T-H. Hubert Chan (HKU), and Elaine Shi (UMD)







### **US Government Investment in MPC:**

NSF: ~\$25M

DARPA: ~\$25M

AFOSR: ~\$15M

IARPA, NSA: ? M

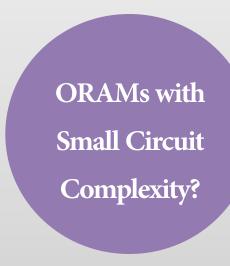
[Gordon et al. 13], [Gentry et al. 13], [Liu et al. 13], [Gentry et al. 14], [Wang et al. 14], etc.



### ORAM has been optimized for a wrong metric.

w.r.t. secure computation

Traditional metric: bandwidth overhead Metric for secure computation: Circuit Size



## Circuit ORAM achieves O(D log N) circuit complexity for blocks of size

 $D = \Omega(\log^2 N)$  bits

Smallest circuit size both asymptotically and in practice.



## Circuit ORAM outperforms Path ORAM by 8x - 48x at 1 GB data size.

Speedup depends on what variations of Path ORAM is used.



# ORAM accesses may be securely evaluated potentially at hundreds of accesses/sec for 4 MB data size

(assuming certain offline preparation)

Garbling can be done at 10<sup>8</sup> gates/sec using off-the-shelf modern processors

(not counting other overhead such as OT)



### **Circuit ORAM:**

For any  $0 < \varepsilon < 1$ , any N-word RAM program with block size of  $\Omega(N^{\varepsilon})$  can be simulated obliviously with  $O(\log N)$  runtime blowup, with inverse poly failure probability.

[Goldreich 87, stronger interpretation]:  $\Omega(logN)$  runtime blowup is necessary for any block size and tolerate up to constant failure probability.

### We are currently implementing Circuit ORAM over garbled circuits!

### **Thank You**

wangxiao@cs.umd.edu