Obliv-C: A Simple C Extension for SMC

Samee Zahur
samee@virginia.edu

Project repository: github.com/samee/obliv-c

Sample Stats

Small samples	“hu661AD0.snp” and “hu604D39.snp”
Execution time	8.47 seconds
Circuit size	19,041,149 non-linear gates
Execution rate	2.24 M gates/second

Batcher's Merge

```
void batcherMerge(char* data,size_t n1,size_t n2,size_t w,
                          void (*cmpswap)(void*,void*))
{
   if (n1+n2 <= 1) return;
   int odd = n1%2,i;
   batcherMerge(data,(n1+1)/2,(n2+!odd)/2,w*2,cmpswap);
   batcherMerge(data+w,n1/2,  (n2+odd)/2, w*2,cmpswap);
   for (i=!odd; i+1<n1+n2; i+=2) cmpswap(data+w*i,data+w*(i+1));
}
```

[Batcher '68]

Compare and Swap

```
void cmpSwapInt(obliv int *a,obliv int *b)
{
    obliv if(*b<*a) swapInt(a,b);
}

void qsort(void *base, size_t nmemb, size_t size,
      int (*cmp)(const void *, const void *));
```

Reusing the Wheel

- File I/O
- Pthreads
- Networking
- Crypto libraries

Implementation & Status

80-bit labels, garbled with the half-gates scheme[1], using fixed-key AES ciphers. Over 2.2 M gates/second over LAN.

DH-based set intersection [Huberman et al. '99] for slow networks (experimental).

[1] Samee Zahur, Mike Rosulek, David Evans. Two Halves Make a Whole: Reducing Data Transfer in Garbled Circuits using Half Gates. In Eurocrypt 2015.

Free for Download!

github.com/samee/obliv-c

samee@virginia.edu