A Zero-One Law for Secure Multi-Party Computation with Ternary Outputs

Gunnar Kreitz

KTH – Royal Institute of Technology
gkreitz@kth.se

TCC, Mar 29 2011

KTH Computer Science and Communication

Our main result

Theorem (This paper)

For every n-argument function $f : A_1 \times \ldots \times A_n \rightarrow \mathbb{Z}_3$, f is either n-private, or it requires honest majority (formally: f is $\lfloor (n-1)/2 \rfloor$-private and not $\lceil n/2 \rceil$-private).

KTH Computer Science and Communication

Secure multi-party computation

- Construct protocol to securely implement some functionality
- n parties jointly fill the role of trusted third party
- Here, we work with symmetric secure function evaluation
  - Each party P_i has secret input x_i
  - Want to evaluate a function $f(x_1, x_2, \ldots, x_n)$
  - f has finite domain
  - All parties receive the output (*symmetric*)

KTH Computer Science and Communication

Our model

- In this talk, all our adversaries are passive (honest-but-curious)
  - Dishonest parties follow the protocol specification
- Information-theoretic security
  - Adversary has unlimited computation power
- Private-channels model
  - Parties are connected pairwise with perfectly private channels

Security

- Threshold adversary
  - Can corrupt any subset of parties of size $\leq t$
- Adversary's goal: learn more than what can be deduced from input of corrupted parties + function's output
- If there is protocol for f with threshold t, then we say f is t-private

KTH Computer Science and Communication

Background results

- In our model, all functions are $\lfloor (n-1)/2 \rfloor$-private [BGW'88, CCD'88]
- This is tight, some functions require honest majority (e.g., disjunction)
- But, some functions are n-private (e.g., summation)
- General understanding of limits is still an open problem

The two-party case is known

- Two-party f either not private, or is 1-private (= 2-private)
- An f with *forbidden submatrix* is not private [Bea'89, Kus'89]
- 1-private protocol for f without forbidden submatrix: *decomposition*
- Oblivious Transfer (OT) is not 1-private

KTH Computer Science and Communication

In general, the privacy hierarchy is complete

- For every $\lceil n/2 \rceil \leq t \leq n-2$ there is f which is t-private but not $t+1$-private [CGK'94]
- Construction to show this has f with large range, $2^{t+2}-2$
- Gives that for range $\mathbb{Z}_{14}$, the hierarchy is complete for $n=4$ parties

KTH Computer Science and Communication

Zero-one law of Boolean privacy

- For Boolean functions, a zero-one law exists [CK'91]
- For Boolean f either:
  - f has an embedded OR, or
  - f is a summation, $f = \sum_{i=1}^{n} f_i(x_i)$

KTH Computer Science and Communication

Zero-one law of Boolean privacy

Theorem ([CK'91])

For every n-argument function $f : A_1 \times \ldots \times A_n \rightarrow \mathbb{Z}_2$, f is either n-private, or it requires honest majority (formally: f is $\lfloor(n-1)/2\rfloor$-private and not $\lceil n/2\rceil$-private).

KTH Computer Science and Communication

Our main result

Theorem (This paper)

For every n-argument function $f : A_1 \times \ldots \times A_n \rightarrow \mathbb{Z}_3$, f is either n-private, or it requires honest majority (formally: f is $\lfloor (n-1)/2 \rfloor$-private and not $\lceil n/2 \rceil$-private).

KTH Computer Science and Communication

Context of the result

- Progress on a long-standing open problem
- Somewhat surprising that there is a zero-one structure for $\mathbb{Z}_3$
- Proof along the lines of classic proofs
- With generalizations of the techniques

KTH Computer Science and Communication

Proof ingredients

- Structure lemma for functions with range $\mathbb{Z}_3$
- Two n-private protocols, generalizing summation and decomposition
- Blood, sweat, and tears

Boolean structure lemma

Lemma ([CK'91])

For every n-argument function $f : A_1 \times \ldots \times A_n \rightarrow \mathbb{Z}_2$*, exactly one of the following holds:*

- f *has an embedded* OR
- f *is a sum:* $\sum_{i=1}^{n} f_i(x_i)$

KTH Computer Science and Communication

Our structure lemma

Lemma (Structure lemma)

For every n-argument function $f : A_1 \times \ldots \times A_n \rightarrow \mathbb{Z}_3$*, at least one of the following holds:*

- f *has an embedded* OR
- f *is a permuted sum:* $\pi_{x_n}(\sum_{i=1}^{n-1} f_i(x_i))$
- f *is collapsible*

KTH Computer Science and Communication

Decomposition

- Recall that for two-party computation, there is a complete characterization
- Functions which are *decomposable* are 1-private (=n-private)
- *Collapsible* is a generalization of decomposable

KTH Computer Science and Communication

Drawing functions

1
1
2

Figure: $f(x_1)$

KTH Computer Science and Communication

Drawing functions

1	1	1	1
2	2	3	3
2	2	4	5

Figure: $f(x_1, x_2)$

KTH Computer Science and Communication

Drawing functions

1	1	1	1	1	1	1	1
2	2	3	3	6	7	6	7
2	2	4	5	7	6	7	6

Figure: $f(x_1, x_2, x_3)$

KTH Computer Science and Communication

Decomposition protocol by example

1	1	1	1	1	1	1	1
2	2	3	3	6	7	6	7
2	2	4	5	7	6	7	6

KTH Computer Science and Communication

Decomposition protocol by example

1	1	1	1	1	1	1	1
2	2	3	3	6	7	6	7
2	2	4	5	7	6	7	6

KTH Computer Science and Communication

Decomposition protocol by example

1	1	1	1	1	1	1	1
2	2	3	3	6	7	6	7
2	2	4	5	7	6	7	6

Decomposition protocol by example

1	1	1	1	1	1	1	1
2	2	3	3	6	7	6	7
2	2	4	5	7	6	7	6

KTH Computer Science and Communication

Decomposition protocol by example

1	1	1	1	1	1	1	1
2	2	3	3	6	7	6	7
2	2	4	5	7	6	7	6

KTH Computer Science and Communication

Collapsible functions

0	1	2	2	2	1
1	0	2	2	2	0
2	2	0	0	1	2

Figure: $f(x_1, x_2, x_3)$

KTH Computer Science and Communication

Collapsible functions

0	1	2	2	2	1
1	0	2	2	2	0
2	2	0	0	1	2

Figure: $f(x_1, x_2, x_3)$

0	0	1	1	1	0
0	0	1	1	1	0
1	1	0	0	0	1

Figure: $\sum_{i=1}^{3} f_i(x_i) \mod 2$

Collapsible functions

0	1	2	2	2	1
1	0	2	2	2	0
2	2	0	0	1	2

Figure: $f(x_1, x_2, x_3)$

0	0	1	1	1	0
0	0	1	1	1	0
1	1	0	0	0	1

Figure: $\sum_{i=1}^{3} f_i(x_i) \mod 2$

KTH Computer Science and Communication

Collapsible functions

0	1				1
1	0				0
		0	0	1	

Figure: Partial $f(x_1, x_2, x_3)$

Collapsible functions

$$\begin{array}{ccc|ccc} 0 & 1 & & & & 1 \\ 1 & 0 & & & & 0 \\ & & 0 & 0 & 1 & \end{array}$$

Figure: Partial $f(x_1, x_2, x_3)$

$$\begin{array}{ccc|ccc} 0 & 2 & 3 & 3 & 1 & 2 \\ 2 & 0 & 1 & 1 & 3 & 0 \\ 1 & 3 & 0 & 0 & 2 & 3 \end{array}$$

Figure: $\sum_{i=1}^{3} f_i(x_i) \mod 4$

Collapsible functions

0	1				1
1	0				0
		0	0	1	

Figure: Partial $f(x_1, x_2, x_3)$

0	2	3	3	1	2
2	0	1	1	3	0
1	3	0	0	2	3

Figure: $\sum_{i=1}^{3} f_i(x_i) \mod 4$

KTH Computer Science and Communication

Blood, Sweat, and Tears

- Structure lemma (case analysis)
- Collapsible functions without embedded OR are n-private
  - Once one output eliminated, remaining two can be separated
- "Large" embedded OR implies "small" embedded OR

To $\mathbb{Z}_4$ and beyond!?

- Do not know if a zero-one law holds for $\mathbb{Z}_4$
- If it does:
  - Protocols and generalized definition still apply for larger ranges
  - But, structure lemma would change
  - Proof heavily relies on range of function

KTH Computer Science and Communication

Conclusions

- Proved Zero-One law for secure computation with range $\mathbb{Z}_3$
- Information-theoretic passive adversary, private channels
- Proof via structure lemma and generalized protocols