A Study of Lower Bounds on Randomness for Three-Party Secure Computation

B. Tech Project I

Srivatsan Sridhar [1]
150070005

Supervised by:
Prof. Sibiraj Pillai [1] Prof. Vinod Prabhakaran [2]

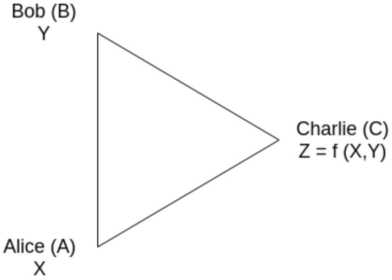
[1]Electrical Engineering
IIT Bombay, India

[2]School of TCS
TIFR Mumbai

November 24, 2018

Three-Party Secure Computation - Introduction

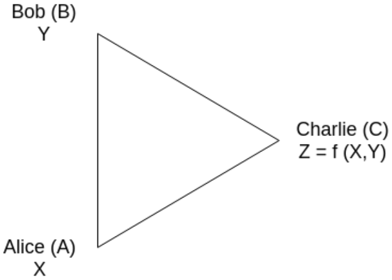
- Alice (A) and Bob (B) have private data X and Y respectively
- Charlie (C) computes a function $Z = f(X, Y)$
- There is a private channel between every pair of parties



Three-Party Secure Computation Model

Three-Party Secure Computation - Objectives

- Charlie must compute Z with zero probability of error
- Charlie must not learn X and Y, more than what Z reveals
- Alice must not learn Y, more than what X reveals
- Bob must not learn X, more than what Y reveals

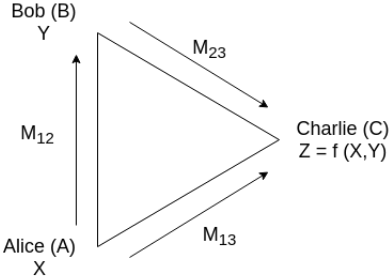


Three-Party Secure Computation Model

Three-Party Secure Computation - One-shot FKN Protocol

1. Alice chooses $M_{12} \in \mathcal{M}_{12}$, sends it to Bob privately
2. Alice sends M_{13}, a function of (M_{12}, X) to Charlie
3. Bob sends M_{23}, a function of (M_{12}, Y) to Charlie
4. Charlie computes $\hat{Z}$ (estimate of Z) as a function of M_{13}, M_{23}

Find minimum $H(M_{12}), H(M_{23}), H(M_{13})$ for this to succeed.



Messages sent in one-shot protocol

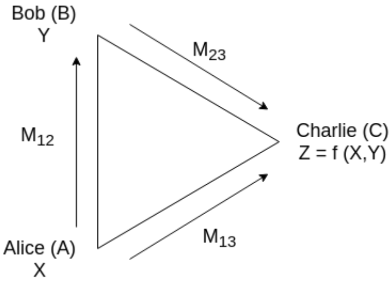
Three-Party Secure Computation - Formal Goals

Secrecy:

- Alice chooses M_{12} independent of X (secrecy for Alice and Bob)
- $(M_{13}, M_{23}) - Z - (X, Y)$ is a Markov Chain (secrecy for Charlie)

Correctness:

- $Pr(\hat{Z} = Z) = 1$ where $\hat{Z}$ is computed by Charlie using M_{13}, M_{23} and $Z = f(X, Y)$.



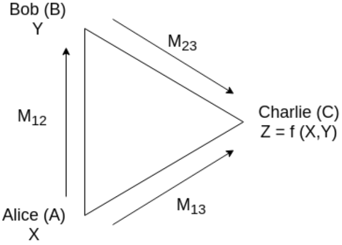
Three-Party Secure Computation Model

Applications of Multi-Party Secure Computation

- **Secure auctions** [1]:
  - N parties bid their highest price for a product
  - Each party's bid to be unknown to other parties and to the seller
  - Seller must correctly determine the highest bidder
- **Benchmark Analysis**:
  - A third party agent compares performance of difference companies based on certain parameters
  - Performance parameters of each company should not be leaked to other companies
- **Machine Learning**:
  - Organization collects data from several users
  - Each user's private data must not be learnt by other users or by the organization
  - Organization must accurately train machine learning models on the data

Secure Computation of AND

- $X, Y \in \{0, 1\}$ and $f(X, Y) = XY$
- Protocol by Feige, Kilian and Naor [2] where:
  - M_{12} is chosen uniformly from $\mathcal{M}_{12}$
  - M_{13} is a deterministic function of (M_{12}, X)
  - M_{23} is a deterministic function of (M_{12}, Y)
  - $H(M_{12}) = log_2 6$ and $H(M_{13}) = H(M_{23}) = log_2 3$
  - Optimal for one-shot protocols without private randomness



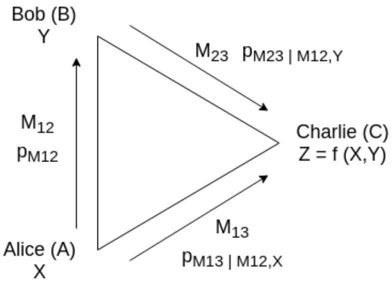
Messages sent in one-shot protocol

Previous Work [3, 4]

- Study of one-shot FKN protocols without private randomness
- Lower bounds for general functions of X and Y
- For AND, $H(M_{13}) \geq log_2 3$ and $|\mathcal{M}_{13}| \geq 3$
- Using the above, and properties of the AND function, $H(M_{12}) \geq log_2 6$ and $|\mathcal{M}_{12}| \geq 6$
- $H(M_{13}) \geq log_2 3$ and $H(M_{12}) \geq 1.826$ when parties are allowed to interact over multiple rounds and use private randomness
- The FKN protocol for AND is optimal for $H(M_{13})$ but may not be for $H(M_{12})$ over more general protocols

Private Randomness

- M_{13} may not a deterministic function of (M_{12}, X).
- M_{13} drawn from a distribution $p_{M_{13}|M_{12},X}$
- There exist functions $f(X, Y)$ where using private randomness decreases the lower bound on $H(M_{12})$
- When can we trade off common randomness for private randomness?



Messages and their distributions

My Work - Proof under Private Randomness

- Can we have $H(M_{12}) < log_2 6$ for secure AND with private randomness?
- **Proof that** $|\mathcal{M}_{12}| \geq 6$ **holds with private randomness too**
- Using two properties of the AND function:
  1. $f(1,1) \neq f(1,0)$. So correctness requires that

     $$supp((M_{13}, M_{23})|XY = 10) \cap supp((M_{13}, M_{23})|XY = 11) = \Phi$$

  2. $f(0,0) = f(0,1) = f(1,0)$. So secrecy requires that

  $$supp((M_{13}, M_{23})|XY = 00) = supp((M_{13}, M_{23})|XY = 01) = supp((M_{13}, M_{23})|XY = 10)$$

- Proof that any $|\mathcal{M}_{12}| < 6$ cannot satisfy these two conditions

My Work - Outline of Proof

- Trivially $|\mathcal{M}_{12}| = 1$ cannot satisfy these conditions
- Suppose that $|\mathcal{M}_{12}| = 3$. Show that this is not possible
- Each cell in the table shows $supp(M_{13}, M_{23}|X, Y, M_{12})$
- $A_1 = supp(M_{13}|X = 0, M_{12} = m_1)$,
  $B_1 = supp(M_{23}|Y = 0, M_{12} = m_1)$
- $A_1 B_1$ denotes set product of A_1 and B_1

	$M_{12} = m_1$	$M_{12} = m_2$	$M_{12} = m_3$
$XY = 00$	$A_1 B_1$	$A_3 B_3$	$A_5 B_5$
$XY = 01$	$A_1 B_2$	$A_3 B_4$	$A_5 B_6$
$XY = 10$	$A_2 B_1$	$A_4 B_3$	$A_6 B_5$
$XY = 11$	$A_2 B_2$	$A_4 B_4$	$A_6 B_6$

My Work - Outline of Proof

1. $f(1,1) \neq f(1,0)$. **Correctness** requires that

$$supp((M_{13}, M_{23})|XY = 10) \cap supp((M_{13}, M_{23})|XY = 11) = \Phi$$

   - Sets in row 4 must be disjoint with the sets in rows 1, 2 or 3

2. $f(0,0) = f(0,1) = f(1,0)$. **Secrecy** requires that

$$supp((M_{13}, M_{23})|XY = 00) = supp((M_{13}, M_{23})|XY = 01) = supp((M_{13}, M_{23})|XY = 10)$$

   - The same sets must appear in rows 1, 2 and 3

	$M_{12} = m_1$	$M_{12} = m_2$	$M_{12} = m_3$
$XY = 00$	A_1B_1	A_3B_3	A_5B_5
$XY = 01$	A_1B_2	A_3B_4	A_5B_6
$XY = 10$	A_2B_1	A_4B_3	A_6B_5
$XY = 11$	A_2B_2	A_4B_4	A_6B_6

My Work - Outline of Proof

- A_1B_2 and A_2B_1 must appear in row 1 (secrecy)
- Elements of A_2 and B_2 cannot appear in the same cell (correctness)

	$M_{12} = m_1$	$M_{12} = m_2$	$M_{12} = m_3$
$XY = 00$	A_1B_1	A_3B_3	A_5B_5
$XY = 01$	A_1B_2	A_3B_4	A_5B_6
$XY = 10$	A_2B_1	A_4B_3	A_6B_5
$XY = 11$	A_2B_2	A_4B_4	A_6B_6

My Work - Outline of Proof

- $A_1 B_2$ and $A_2 B_1$ must appear in row 1 (secrecy)
- Elements of A_2 and B_2 cannot appear in the same cell (correctness)
- We must have $A_1 \subseteq A_3$, $B_2 \subseteq B_3$, $A_2 \subseteq A_5$, $B_1 \subseteq B_5$
- This tells us that $|\mathcal{M}_{12}| = 2$ is not possible
- $B_2 \subseteq B_3 \implies A_2 \cap A_3 = \Phi$ (correctness)
- $B_1 \subseteq B_5 \implies B_1 \cap B_6 = \Phi$ (correctness)
- This means $A_2 B_1$ cannot appear in row 2 (violation of secrecy)
- This violation shows that $|\mathcal{M}_{12}| = 3$ is not possible

	$M_{12} = m_1$	$M_{12} = m_2$	$M_{12} = m_3$
$XY = 00$	$A_1 B_1$	$A_1 B_2$	$A_2 B_1$
$XY = 01$	$A_1 B_2$	$A_1 B_4$	$A_2 B_6$
$XY = 10$	$A_2 B_1$	$A_4 B_2$	$A_6 B_5$
$XY = 11$	$A_2 B_2$	$A_4 B_4$	$A_6 B_6$

My Work - Outline of Proof

- Continue similarly to prove that $|\mathcal{M}_{12}| = 4, 5$ are not possible
- All possible assignments of sets fail the two conditions
- Thus $|\mathcal{M}_{12}| \geq 6$ is required
- **Next question** - Can we have $H(M_{12}) < log_2 6$?
- $|\mathcal{M}_{12}| \geq 6$ does not imply that $H(M_{12}) \geq log_2 6$

Further Work

- Can we have $H(M_{12}) < log_2 6$ with private randomness?
- Only looked at supports of messages so far
- Take into account properties of the distributions
- Generalizing the two properties of AND as:
  1. $f(1,1) \neq f(1,0)$. So correctness requires that

     $$supp((M_{13}, M_{23})|XY = 10) \cap supp((M_{13}, M_{23})|XY = 11) = \Phi$$

  2. $f(0,0) = f(0,1) = f(1,0)$. So secrecy requires that

     $$\begin{gathered} Pr((M_{13}, M_{23}) = (a,b)|XY = 00) = \\ Pr((M_{13}, M_{23}) = (a,b)|XY = 01) = \\ Pr((M_{13}, M_{23}) = (a,b)|XY = 10) \end{gathered}$$

References I

[1] R. Cramer, I. B. Damgrd, and J. B. Nielsen, *Secure Multiparty Computation and Secret Sharing*.
New York, NY, USA: Cambridge University Press, 1st ed., 2015.

[2] U. Feige, J. Killian, and M. Naor, "A minimal model for secure computation (extended abstract)," in *Proceedings of the Twenty-sixth Annual ACM Symposium on Theory of Computing*, STOC '94, (New York, NY, USA), pp. 554–563, ACM, 1994.

[3] S. R. S, S. Rajakrishnan, A. Thangaraj, and V. Prabhakaran, "Lower bounds and optimal protocols for three-party secure computation," in *2016 IEEE International Symposium on Information Theory (ISIT)*, pp. 1361–1365, July 2016.

[4] D. Data, V. M. Prabhakaran, and M. M. Prabhakaran, "Communication and randomness lower bounds for secure computation," *CoRR*, vol. abs/1512.07735, 2015.

Thank You!

Questions?