Communication and Randomness Lower Bounds for Secure Multiparty Computation

B. Tech Project

Srivatsan Sridhar
150070005

Supervised by:

Prof. Sibiraj Pillai
Electrical Engineering, IIT Bombay

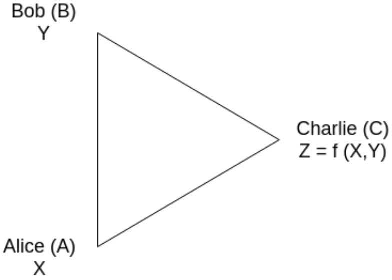
Prof. Vinod Prabhakaran
School of TCS, TIFR Mumbai

Prof. Manoj Prabhakaran
Computer Science and Engineering, IIT Bombay

May 9, 2019

Three-Party Secure Computation - Introduction

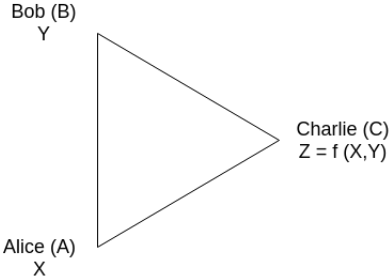
- Alice (A) and Bob (B) have private data X and Y respectively
- Charlie (C) computes a function $Z = f(X, Y)$
- There is a private channel between every pair of parties



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 and Z, more than what X reveals
- Bob must not learn X and Z, more than what Y reveals

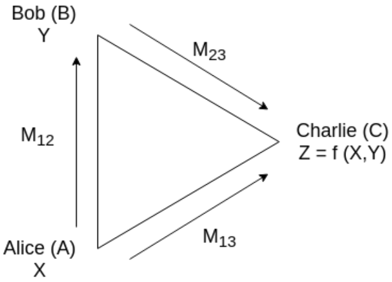


Three-Party Secure Computation Model

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

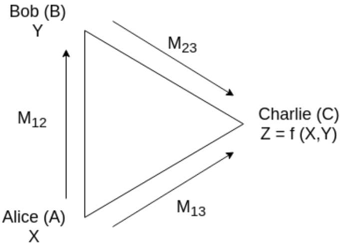
Three-Party Secure Computation - Formal Goals

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)
  or $Pr(m_{13}, m_{23}|x, y) = Pr(m_{13}, m_{23}|x', y')$
  if $f(x, y) = f(x', y')$

Correctness:

- $\text{supp}(M_{13}, M_{23}|x, y) \cap \text{supp}(M_{13}, M_{23}|x'y') = \Phi$
  if $f(x, y) \neq f(x', y')$

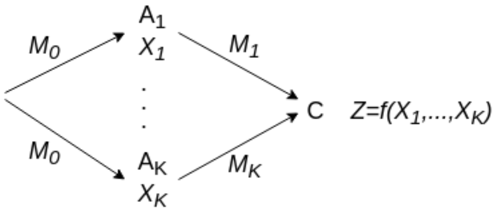


Three-Party Secure Computation Model

Multiparty Secure Computation - Extended FKN Protocol

Parties $\mathsf{A}_1, \ldots, \mathsf{A}_k$ with inputs $X_1, \ldots, X_k$

1. Common randomness $M_0 \in \mathcal{M}_0$ given to parties $\mathsf{A}_1, \ldots, \mathsf{A}_k$
2. Each party sends M_i, a function of (M_0, X_i) to Charlie
3. Charlie computes $\widehat{Z}$ as a function of $(M_1, \ldots, M_k)$



Multiparty Secure Computation Model

Applications of Multi-Party Secure Computation

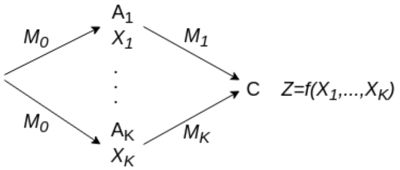
- **Secure Audio Teleconferencing**:
  - Bridge mediates communication by detecting which party's signal has the maximum amplitude
  - Compute max of encrypted signals without decrypting them
- **Secure auctions**:
  - N parties bid their price for a product
  - Each party's bid to be unknown to other 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
  - Accurately train machine learning models on the data

Literature Study - Existence of Secure Protocols

- Feige, Kilian, Naor (1994) proved that secure computation protocol exists for any function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$
- Amount of communication and randomness may be exponential in input length
- Communication and randomness polynomial if f is in *nondeterministic logspace*
- Protocol for secure multiparty computation of logical AND

Secure Computation of AND - Multiparty Protocol

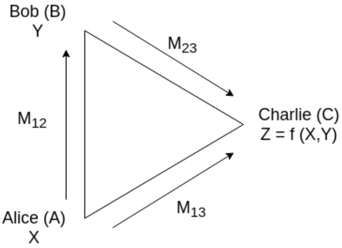
- $X_1, \ldots, X_k \in \{0,1\}$ and $f(X_1, \ldots, X_k) = X_1 \wedge \ldots \wedge X_k$
- Protocol by Feige, Kilian and Naor where:
  - Choose a prime $p > k$
  - M_0 is $0 < r < p$ and $r_1, \ldots, r_k$ with $\sum_{i=1}^{k} r_i = 0 \bmod p$
  - Each party sends $M_i = r(1 - x_i) + r_i \bmod p$ if its input is x_i
  - Charlie outputs $Z = 1$ iff $\sum_{i=1}^{k} M_i = 0 \bmod p$
- Cardinality of $|\mathcal{M}_0| = p^{k-1}(p-1)^k$ and $|\mathcal{M}_i| = p$



One-shot protocol for multiparty AND

Secure Computation of AND - Three-party Protocol

- $X, Y \in \{0, 1\}$ and $f(X, Y) = X \wedge Y$
- Protocol by Feige, Kilian and Naor where:
  - M_{12} is a random permutation of $(0, 1, 2)$, say (α, β, γ)
  - Alice sends $M_{13} = \alpha$ if $X = 1$ and β if $X = 0$
  - Bob sends $M_{23} = \alpha$ if $Y = 1$ and γ if $Y = 0$
  - Charlie computes $Z = 1$ if $M_{13} = M_{23}$, and $Z = 0$ otherwise
- Cardinality of $|\mathcal{M}_{12}| = 6$ and $|\mathcal{M}_{13}| = |\mathcal{M}_{23}| = 3$



One-shot protocol for three-party AND

Literature Study - Existing Bounds

- Information theoretic bounds for general functions, using interactive protocols with private randomness. For AND,

$$H(M_{13}) \geq \log_2 3,\ \ H(M_{23}) \geq \log_2 3 \text{ and } H(M_{12}) \geq 1.826$$

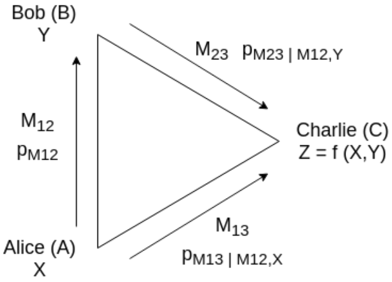
- Given protocol : $H(M_{13}), H(M_{23}) = \log_2 3$ and $H(M_{12}) = \log_2 6$
- Common randomness lower bound not achieved by the protocol
- For one-shot protocols without private randomness (e.g. FKN),

$$H(M_{13}) \geq \log_2 3,\ \ H(M_{23}) \geq \log_2 3 \text{ and } H(M_{12}) \geq \log_2 6$$

- 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 $H(M_{12})$
- Can we trade off common randomness for private randomness?



Messages and their distributions

Private Randomness - Example of Protocol

Consider the following function with $X, Y \sim \text{Unif}\{0, 1, 2\}$:

$$f(X, Y) = \begin{cases} 2 & \text{if } X = 2 \text{ or } Y = 2 \\ X \oplus Y & \text{otherwise} \end{cases}$$

Protocol with k' and k'' drawn from Alice's and Bob's private randomness

1. M_{12} contains a uniformly chosen permutation of $(0, 1, 2)$, say (α, β, γ) and a uniform bit k.
2. Alice sends $M_{13} = (\alpha, X \oplus k)$ if $X \in \{0, 1\}$, and (β, k') if $X = 2$.
3. Bob sends $M_{23} = (\alpha, Y \oplus k)$ if $Y \in \{0, 1\}$, and (γ, k'') if $Y = 2$.
4. Charlie finds $Z = 2$ if $M_{13}(1) = M_{23}(1)$, and $Z = M_{13}(2) \oplus M_{23}(2)$ otherwise.

Private Randomness - Example of Protocol

Consider the following function with $X, Y \sim \text{Unif}\{0, 1, 2\}$:

$$f(X, Y) = \begin{cases} 2 & \text{if } X = 2 \text{ or } Y = 2 \\ X \oplus Y & \text{otherwise} \end{cases}$$

Theoretical bounds without private randomness :

$$H(M_{13}) \geq 2.3137,\ H(M_{23}) \geq 2.3137 \text{ and } H(M_{12}) \geq 3.8987$$

Achieved by the protocol :

$$H(M_{13}) = H(M_{23}) = \log_2 3 + 1 \approx 2.5850$$
$$H(M_{12}) = \log_2 6 + 1 \approx 3.5850$$

My Work - Proof under Private Randomness

- $|\mathcal{M}_{12}| \geq 6$ **holds for non-interactive protocols with private randomness for secure computation of AND**
- Using two properties of the AND function:
  1. $f(1,1) \neq f(1,0)$. So correctness requires that

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

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

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

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

Proof - Private Randomness by One Party

- Suppose only Bob uses private randomness.
- Fix $M_{12} = m_{12}$ and let $a = m_{13}(m_{12}, 0)$. Let

$$
\begin{aligned}
& b \in \mathrm{supp}(M_{23} | Y = 0, M_{12} = m_{12}), \\
& b' \in \mathrm{supp}(M_{23} | Y = 1, M_{12} = m_{12}) \\
\implies & [a, b] \in \mathrm{supp}((M_{13}, M_{23}) | XY = 00)
\end{aligned}
$$

- From the condition for secrecy,

$$[a, b'] \in \mathrm{supp}((M_{13}, M_{23}) | XY = 00)$$

- For every a in $\mathrm{supp}(M_{13}|X = 0)$, there exists $m_{12}, m'_{12} \in \mathcal{M}_{12}$ such that $a = m_{13}(m_{12}, 0) = m_{13}(m'_{12}, 0)$
-
$$|\mathcal{M}_{12}| \geq 2|\mathrm{supp}(M_{13}|X = 0)| = 2|\mathrm{supp}(M_{13})| \geq 6$$

Proof - Private Randomness by Both Parties

- Each row represents an input combination
- Each column represents one value of the common randomness
- Each cell in the table shows $supp(M_{13}, M_{23}|X, Y, M_{12})$
- $A_1^0 = supp(M_{13}|X = 0, M_{12} = 1)$,
  $B_1^0 = supp(M_{23}|Y = 0, M_{12} = 1)$
- $A_1^0 B_1^0$ denotes set product of A_1^0 and B_1^0

	$M_{12} = 1$	$M_{12} = 2$	$M_{12} = 3$	$M_{12} = 4$	$M_{12} = 5$	$M_{12} = 6$
$XY = 00$	$A_1^0 B_1^0$	$A_2^0 B_2^0$	$A_3^0 B_3^0$	$A_4^0 B_4^0$	$A_5^0 B_5^0$	$A_6^0 B_6^0$
$XY = 01$	$A_1^0 B_1^1$	$A_2^0 B_2^1$	$A_3^0 B_3^1$	$A_4^0 B_4^1$	$A_5^0 B_5^1$	$A_6^0 B_6^1$
$XY = 10$	$A_1^1 B_1^0$	$A_2^1 B_2^0$	$A_3^1 B_3^0$	$A_4^1 B_4^0$	$A_5^1 B_5^0$	$A_6^1 B_6^0$
$XY = 11$	$A_1^1 B_1^1$	$A_2^1 B_2^1$	$A_3^1 B_3^1$	$A_4^1 B_4^1$	$A_5^1 B_5^1$	$A_6^1 B_6^1$

Proof - Private Randomness by Both Parties

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

Proof - Private Randomness by Both Parties

- For secrecy, we need at least $|\mathcal{M}_{12}| \geq 2$
- For $|\mathcal{M}_{12}| = 2$, we need $A_1^0 B_1^1 \subseteq A_2^0 B_2^0$ and $A_1^1 B_1^0 \subseteq A_2^0 B_2^0$
- $A_1^0, A_1^1 \subseteq A_2^0$ and $B_1^1, B_1^0 \subseteq B_2^0 \implies A_1^1 B_1^1 \subseteq A_2^0 B_2^0$ (Contradiction)

	$M_{12} = 1$	$M_{12} = 2$	$M_{12} = 3$	$M_{12} = 4$	$M_{12} = 5$	$M_{12} = 6$
$XY = 00$	$A_1^0 B_1^0$	$A_2^0 B_2^0$ $(A_1^1 B_1^0)$ $(A_1^0 B_1^1)$	$A_3^0 B_3^0$	$A_4^0 B_4^0$	$A_5^0 B_5^0$	$A_6^0 B_6^0$
$XY = 01$	$A_1^0 B_1^1$	$A_2^0 B_2^1$	$A_3^0 B_3^1$	$A_4^0 B_4^1$	$A_5^0 B_5^1$	$A_6^0 B_6^1$
$XY = 10$	$A_1^1 B_1^0$	$A_2^1 B_2^0$	$A_3^1 B_3^0$	$A_4^1 B_4^0$	$A_5^1 B_5^0$	$A_6^1 B_6^0$
$XY = 11$	$A_1^1 B_1^1$	$A_2^1 B_2^1$	$A_3^1 B_3^1$	$A_4^1 B_4^1$	$A_5^1 B_5^1$	$A_6^1 B_6^1$

Proof - Private Randomness by Both Parties

- WLOG, assume

$$A_1^1 \cap A_2^0 \neq \Phi,\ B_1^0 \cap B_2^0 \neq \Phi,\ A_1^0 \cap A_3^0 \neq \Phi,\ B_1^1 \cap B_3^0 \neq \Phi$$

$$B_1^1 \cap B_2^0 = \Phi,\ B_1^1 \cap B_2^1 = \Phi,\ A_1^1 \cap A_3^0 = \Phi,\ A_1^1 \cap A_3^1 = \Phi$$

	$M_{12} = 1$	$M_{12} = 2$	$M_{12} = 3$	$M_{12} = 4$	$M_{12} = 5$	$M_{12} = 6$
$XY = 00$	$A_1^0 B_1^0$	$A_2^0 B_2^0$ $(A_1^1 B_1^0)$	$A_3^0 B_3^0$ $(A_1^0 B_1^1)$	$A_4^0 B_4^0$	$A_5^0 B_5^0$	$A_6^0 B_6^0$
$XY = 01$	$A_1^0 B_1^1$	$A_2^0 B_2^1$	$A_3^0 B_3^1$	$A_4^0 B_4^1$	$A_5^0 B_5^1$	$A_6^0 B_6^1$
$XY = 10$	$A_1^1 B_1^0$	$A_2^1 B_2^0$	$A_3^1 B_3^0$	$A_4^1 B_4^0$	$A_5^1 B_5^0$	$A_6^1 B_6^0$
$XY = 11$	$A_1^1 B_1^1$	$A_2^1 B_2^1$	$A_3^1 B_3^1$	$A_4^1 B_4^1$	$A_5^1 B_5^1$	$A_6^1 B_6^1$

Proof - Private Randomness by Both Parties

- $A_1^1 \cap A_4^0 = A_1^1 \cap A_5^0 = \Phi$ or $A_1^1 \cap A_4^0 \neq \Phi, A_1^1 \cap A_5^0 \neq \Phi$ lead to a contradiction
- WLOG also assume

$$A_1^1 \cap A_4^0 \neq \Phi,\ A_1^1 \cap A_5^0 = \Phi,\ B_1^1 \cap B_4^0 = \Phi,\ B_1^1 \cap B_5^0 \neq \Phi$$

	$M_{12} = 1$	$M_{12} = 2$	$M_{12} = 3$	$M_{12} = 4$	$M_{12} = 5$	$M_{12} = 6$
$XY = 00$	$A_1^0 B_1^0$	$A_2^0 B_2^0$ $(A_1^1 B_1^0)$	$A_3^0 B_3^0$ $(A_1^0 B_1^1)$	$A_4^0 B_4^0$ $(A_1^1 B_1^0)$	$A_5^0 B_5^0$ $(A_1^0 B_1^1)$	$A_6^0 B_6^0$
$XY = 01$	$A_1^0 B_1^1$	$A_2^0 B_2^1$	$A_3^0 B_3^1$	$A_4^0 B_4^1$	$A_5^0 B_5^1$	$A_6^0 B_6^1$
$XY = 10$	$A_1^1 B_1^0$	$A_2^1 B_2^0$	$A_3^1 B_3^0$	$A_4^1 B_4^0$	$A_5^1 B_5^0$	$A_6^1 B_6^0$
$XY = 11$	$A_1^1 B_1^1$	$A_2^1 B_2^1$	$A_3^1 B_3^1$	$A_4^1 B_4^1$	$A_5^1 B_5^1$	$A_6^1 B_6^1$

Proof - Private Randomness by Both Parties

- Enumerate all valid ways of splitting elements of $A_1^1 B_1^0$ in columns 2 and 4 and $A_1^0 B_1^1$ in columns 3 and 5
- For each case, assign other sets as per correctness and secrecy conditions
- Show that each of these cases leads to a contradiction

	$M_{12} = 1$	$M_{12} = 2$	$M_{12} = 3$	$M_{12} = 4$	$M_{12} = 5$	$M_{12} = 6$
$XY = 00$	$A_1^0 B_1^0$	$A_2^0 B_2^0$ $(A_1^1 B_1^0)$	$A_3^0 B_3^0$ $(A_1^0 B_1^1)$	$A_4^0 B_4^0$ $(A_1^1 B_1^0)$	$A_5^0 B_5^0$ $(A_1^0 B_1^1)$	$A_6^0 B_6^0$
$XY = 01$	$A_1^0 B_1^1$	$A_2^0 B_2^1$	$A_3^0 B_3^1$	$A_4^0 B_4^1$	$A_5^0 B_5^1$	$A_6^0 B_6^1$
$XY = 10$	$A_1^1 B_1^0$	$A_2^1 B_2^0$	$A_3^1 B_3^0$	$A_4^1 B_4^0$	$A_5^1 B_5^0$	$A_6^1 B_6^0$
$XY = 11$	$A_1^1 B_1^1$	$A_2^1 B_2^1$	$A_3^1 B_3^1$	$A_4^1 B_4^1$	$A_5^1 B_5^1$	$A_6^1 B_6^1$

Entropy Bound - Private Randomness by Both Parties

- Proved that $|\mathcal{M}_{12}| \geq 6$ for non-interactive protocols with private randomness
- Next step : Prove $H(M_{12}) \geq \log_2 6$ for the same class of protocols
- Let $x \in \mathcal{X}$ and $S_x \subseteq \mathcal{Y}$ such that $f(x,y) = f(x,y')$ for all $y, y' \in S_x$
- Without private randomness, it is known that (with $x = 0$)

$$H(M_{12}) \geq H(M_{13}|X = x) + \log_2 |S_x| = H(M_{13}) + 1 \geq \log_2 3 + 1$$

- **Proved that with private randomness**,

$$H(M_{12}) \geq I(M_{12}; M_{13}|X = x) + \log_2 |S_x|$$

Proof - Entropy Bound with Private Randomness

- Let $x \in \mathcal{X}$, $S_x = \{y_1, \ldots y_{|S_x|}\}$, and $m_{12} \in \mathcal{M}_{12}$ such that

$$[a, b_i] \in \text{supp}((M_{13}, M_{23})|m_{12}, x, y_i)$$

- From the secrecy condition,

$$Pr(M_{13} = a, M_{23} = b_i|x, y_i) = Pr(M_{13} = a, M_{23} = b_i|x, y_1)$$

- First show that

$$Pr(M_{13} = a|x) \geq |S_x| \; Pr(M_{12} = m_{12}) Pr(M_{13} = a|m_{12}, x)$$

and hence whenever $a \in \text{supp}(M_{13}|M_{12} = m_{12}, X = x)$,

$$p(m_{12}) \leq \frac{p(a|x)}{|S_x| \; p(a|m_{12}, x)}$$

Proof - Entropy Bound with Private Randomness

Denote $\mathrm{supp}(M_{23}|m_{12}, y_i)$ as B_i

$$Pr(M_{13} = a|x) = Pr(M_{13} = a|x, y_1)$$

$$\geq \sum_{i=1}^{|S_x|} \sum_{b \in B_i} Pr(M_{13} = a, M_{23} = b|x, y_1)$$

$$= \sum_{i=1}^{|S_x|} \sum_{b \in B_i} Pr(M_{13} = a, M_{23} = b|x, y_i)$$

$$= \sum_{i=1}^{|S_x|} \sum_{b \in B_i} \sum_{m \in \mathcal{M}_{12}} Pr(M_{12} = m) Pr(M_{13} = a|m, x) Pr(M_{23} = b|m, y_i)$$

$$\geq \sum_{i=1}^{|S_x|} \sum_{b \in B_i} Pr(M_{12} = m_{12}) Pr(M_{13} = a|m_{12}, x) Pr(M_{23} = b|m_{12}, y_i)$$

$$= |S_x| \; Pr(M_{12} = m_{12}) Pr(M_{13} = a|m_{12}, x)$$

Proof - Entropy Bound with Private Randomness

Denote $\text{supp}(M_{13}|M_{12} = m, X = x)$ as $A(m, x)$ and $\text{supp}(M_{13}|X = x)$ as $A(x)$

$$H(M_{12}) = \sum_{m \in \mathcal{M}_{12}} p(m) \log_2 \left(\frac{1}{p(m)} \right)$$

$$= \sum_{m \in \mathcal{M}_{12}} \sum_{a \in A(m,x)} p(a|m, x) p(m) \log_2 \left(\frac{1}{p(m)} \right)$$

$$\geq \sum_{m \in \mathcal{M}_{12}} \sum_{a \in A(m,x)} p(a|m, x) p(m) \log_2 \left(\frac{|S_x| \; p(a|m, x)}{p(a|x)} \right)$$

$$= \sum_{a \in A(x)} \sum_{m \in \mathcal{M}_{12}} p(a|m, x) p(m) \log_2 \left(\frac{|S_x|}{p(a|x)} \right) - p(a|m, x) p(m) \log_2 \left(\frac{1}{p(a|m, x)} \right)$$

$$= \log_2 |S_x| + \sum_{a \in A(x)} p(a|x) \log_2 \left(\frac{1}{p(a|x)} \right) - \sum_{m \in \mathcal{M}_{12}} p(m) H(M_{13}|m, x)$$

$$= \log_2 |S_x| + H(M_{13}|X = x) - H(M_{13}|M_{12}, X = x)$$

$$= I(M_{12}; M_{13}|X = x) + \log_2 |S_x|$$

Proof - Entropy Bound with Private Randomness

- Evaluating the bound

$$H(M_{12}) \geq I(M_{12}; M_{13}|X = x) + \log_2|S_x|$$

- For the protocol with randomness

$$H(M_{12}) \geq I(M_{12}; M_{13}|X = x)+\log_2|S_x| = \log_2 3+\log_2 3 = \log_2 9$$

- The protocol uses $H(M_{12}) = \log_2 12$
- For AND, choosing $x = 0$ and $S_x = \{0, 1\}$

$$H(M_{12}) \geq I(M_{12}; M_{13}|X = x) + 1$$

- It is not clear how to evaluate $I(M_{12}; M_{13}|X = x)$ in terms of input distributions

Relation with Distribution Design

- Problem motivated by secure multiparty computation, scret sharing
- Design a joint distribution on a set of random variables $X_1, \ldots, X_n$, that satisfies a set of constraints.
- Two types of constraints on sets of random variables $(X_{i_1}, \ldots, X_{i_d})$ and $(X_{i'_1}, \ldots, X_{i'_d})$
  - They have identical joint distributions

$$(X_{i_1}, \ldots, X_{i_d}) \equiv (X_{i'_1}, \ldots, X_{i'_d})$$

  - They have disjoint support sets

$$(X_{i_1}, \ldots, X_{i_d}) \parallel (X_{i'_1}, \ldots, X_{i'_d})$$

Distribution Design - Secure Computation of AND

Random Variables :

- M_{13}^0, M_{13}^1 : Messages sent by Alice for inputs 0 and 1
- M_{23}^0, M_{23}^1 : Messages sent by Bob for inputs 0 and 1

Constraints :

$$(M_{13}^0, M_{23}^0) \equiv (M_{13}^0, M_{23}^1) \equiv (M_{13}^1, M_{23}^0)$$
$$(M_{13}^1, M_{23}^1) \parallel (M_{13}^0, M_{23}^0)$$
$$(M_{13}^1, M_{23}^1) \parallel (M_{13}^0, M_{23}^1)$$
$$(M_{13}^1, M_{23}^1) \parallel (M_{13}^1, M_{23}^0)$$

Use Lemma : $A_0 \subseteq [n], 0 < |A_0| = d < n$. Consider the constraints $\{A \parallel A_0 \,:, A \subseteq [n], |A| = d, A \neq A_0\} \cup$ $\{A \equiv A' \,:\, A, A' \subseteq [n], |A| = |A'| = d, A, A' \neq A_0\}$.
Then there exists a distribution design with $\lceil \log_2 |\mathrm{supp}(X_i)| \rceil$ at most $\min\{2d \cdot \log_2 n, n-1\}$

Distribution Design - Result and Limitations

Result :

- Distribution design exists for secure AND with $|\text{supp}(M_{13})| = |\text{supp}(M_{13}^0)| = |\text{supp}(M_{13}^1)|$ at most 8
- For AND of k parties, $|\text{supp}(M_i)|$ at most 2^{2k-1}

Limitations :

- Known protocol requires only $|\text{supp}(M_i)| \sim O(k)$
- Used lemma includes unnecessary constraints of the form

$$(M_{13}^0, M_{13}^1) \,\|\, (M_{13}^1, M_{23}^1) \text{ and } (M_{13}^0, M_{13}^1) \equiv (M_{13}^0, M_{23}^0)$$

- Proof of lemma uses construction that may not be optimal in general
- Does not explicitly use the common randomness variables

Distribution Design - Secure Multiparty Computation

- Formulate secure multiparty computation of any function $f : \mathcal{X}_1 \times \ldots \times \mathcal{X}_k \to \{0, 1\}$ as a distribution design
- Optimal bounds for distribution design will also solve secure multiparty computation
- Choose the random variables $\{M_i^x : x \in \mathcal{X}_i, i = 1, \ldots, n\}$, and the constraints as

$$
\begin{aligned}
(M_1^{x_1}, \ldots, M_k^{x_k}) &\equiv (M_1^{x_1'}, \ldots, M_k^{x_k'}) \quad \text{if } f(x_1, \ldots, x_k) = f(x_1', \ldots, x_k') \\
(M_1^{x_1}, \ldots, M_k^{x_k}) &\parallel (M_1^{x_1'}, \ldots, M_k^{x_k'}) \quad \text{if } f(x_1, \ldots, x_k) \neq f(x_1', \ldots, x_k')
\end{aligned}
$$

Future Work

- Generic bounds that can extend to functions other than AND as well
- Formalize the counting argument proof in a systematic way
- Entropy bounds - Evaluating $I(M_{12}; M_{13}|X = x)$ for general functions
- Extending entropy bounds to multiparty secure computation
- Analyzing this problem as a distribution design problem, with added constraints for using the common randomness variables.
- Alternately, consider a support design problem

References I

[1] 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.

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

[3] 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.

[4] 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.

[5] A. Beimel, A. Gabizon, Y. Ishai, and E. Kushilevitz, "Distribution design," in *Proceedings of the 2016 ACM Conference on Innovations in Theoretical Computer Science*, ITCS '16, (New York, NY, USA), pp. 81–92, ACM, 2016.

[6] R. Heiman, "Secure audio teleconferencing: A practical solution," in *Advances in Cryptology — EUROCRYPT' 92* (R. A. Rueppel, ed.), (Berlin, Heidelberg), pp. 437–448, Springer Berlin Heidelberg, 1993.

Thank You!
Questions?