Secure Multi-Party Computation – Lower Bounds and Optimal Protocols

A Project Report

submitted by

SUNDARA RAJAN S

in partial fulfilment of the requirements
for the award of the degree of

BACHELOR OF TECHNOLOGY AND MASTER OF TECHNOLOGY

DEPARTMENT OF ELECTRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY MADRAS.

May 2016

THESIS CERTIFICATE

This is to certify that the thesis titled **Secure Multi-Party Computation – Lower Bounds and Optimal Protocols**, submitted by **Sundara Rajan S**, to the Indian Institute of Technology, Madras, for the award of the degree of **Bachelor of Technology and Master of Technology**, is a bona fide record of the research work done by him under our supervision. The contents of this thesis, in full or in parts, have not been submitted to any other Institute or University for the award of any degree or diploma.

Prof. Andrew Thangaraj
Research Guide
Professor
Dept. of Electrical Engineering
IIT Madras, 600 036

Prof. Vinod Prabhakaran
Research Guide
Reader
School of Tech. and Computer Science
TIFR, Mumbai 400 005

Place: Chennai

Date: 20th May 2016

ACKNOWLEDGEMENTS

I would like to convey my heartfelt gratitude to my advisors – Prof. Andrew Thangaraj and Prof. Vinod Prabhakaran – for introducing me to research and being great mentors; I could not have asked for more. I would also like to thank my friend and research partner Shijin Rajakrishnan for being a great collaborator. I am highly indebted to the faculty of IIT Madras, under whom I took courses, for their sincere effort to disseminate knowledge; it definitely has been a privilege sitting in many of their classes. I would like to thank my faculty advisor Prof. C. S. Ramalingam, for his caring mentorship during my stay at IIT Madras. I would like to thank all my friends at IIT Madras for an enjoyable and unforgettable 5 years. I would like to thank the entire IITM ecosystem – from the people who help keep the campus clean, to the monkeys which are a great source of entertainment – for providing me with the most comfortable and fun environment. Lastly, but most importantly, I cannot thank my parents and my brother enough, for being the best family I could possibly ask for, and without whom I would never be the person I am today.

ABSTRACT

KEYWORDS: Information theory, Information and data security, Cryptography, Communication complexity, Secure function computation, 2-transitive permutation sets

The paramount importance of information security and privacy can not be overemphasized in the modern data-driven society. In this work, we study one aspect of information-security, namely – secure multi-party computation. Our concept of security is information-theoretic as opposed to security relying on computational hardness assumptions. The problem of three-party secure computation, where a function of private data of two parties is to be computed by a third party without revealing information beyond respective inputs or outputs is considered. New and better lower bounds on the amount of communication required between the parties to guarantee zero probability of error in the computation and achieve information-theoretic security are derived. Protocols are presented and proved to be optimal in some cases by showing that they achieve the improved lower bounds.

TABLE OF CONTENTS

LIST OF PROTOCOLS

LIST OF FIGURES

ABBREVIATIONS

IITM	Indian Institute of Technology, Madras
MPC	Multi-party computation
EQ	Equality function
FKN	The work of Feige, Kilian, and Naor (Feige u. a., 1994)

NOTATION

X	A random variable
$\mathcal{X}$	Alphabet of a random variable
supp(X)	Support set of X
$H(X)$	Shannon entropy of X
$I(X;Y)$	Mutual information between X and Y
$X-Y-Z$	A Markov chain
$RI(X;Y)$	Residual information between X and Y

CHAPTER 1

INTRODUCTION

The paramount importance of information security and privacy can not be overemphasized in the modern data-driven society. Organizations like Google, Facebook and Microsoft's servers handle thousands of pentabytes of data every month. With the humongous volume of data flowing in the giant web of internet, the potential danger of bank details, payment information, client profiles and personal files getting lost or falling into the wrong hands looms large.

Cryptography, a sub-field of theoretical computer science, concerns itself with the study of hiding information from third parties called adversaries. Cryptographers and cryptanalysts have for years constructed and analysed protocols that prevent third parties from accessing private information. While the majority of cryptographic protocols – designed over unproven computational hardness assumptions – are easy to implement and reasonably effective for day-to-day purposes, there are two critical drawbacks concerning their usage:

1. Theoretical advances in areas like number theory (integer factorization, for e.g.) would demand adaptability of these algorithms.

2. They are particularly vulnerable to emerging technological developments like quantum computing.

Information theoretic security is an aspect of cryptography which circumvents the aforementioned problems of the modern cryptographic protocols. Information theoretically cryptographic protocols do not rely on computational hardness assumptions and are invulnerable to quantum computing advancements because of the inherent definition of security and privacy in such protocols. The seminal work of Shannon (Shannon, 1949) introduced the concept of information-theoretic security. The obvious disadvantage of these protocols is the difficulty in implementing them on a large scale (see Orlandi (2011) for recent advances in implementations for multi-party computation in general). Neverthe-

less, information-theoretically secure cryptosystems are largely used for the most sensitive governmental and military communications.

A variety of tasks exist for which information-theoretic security is meaningful:

1. Secret Sharing schemes, like that of Shamir's (check Appendix A for the scheme), are information-theoretically secure.

2. Private information retrieval with multiple databases can be achieved with information-theoretic privacy for the user's query.

3. Quantum cryptographic protocols are mostly information-theoretically secure.

4. Secure multi-party computation (MPC), the superset of this thesis topic, often (but not necessarily) concerns with information-theoretic security.

1.1 Information-Theoretically Secure Multi-Party Computation (MPC)

MPC is a very general and one of the most important problems in cryptography. In our modern, highly data-driven systems and networks, individuals and organizations often interact directly and indirectly with a large number of parties. In such a complex scenario, it is imperative that one must keep their private data *as confidential as possible*. Of course, one could store their data in a hardware device and lock it away, but that would undermine the very value of the data – to be of some use. A very interesting case that often arises and that makes MPC relevant is that it is possible to combine *confidential information* from several sources to churn out some result of value to all the parties. To illustrate what we mean by this, consider the following real-world scenario, verbatim from Cramer u. a. (2012) (see there for a comprehensive treatment of MPC):

1.1.1 Auctions

Auctions exist in many variants and are used for all kinds of purposes, but we concentrate here on the simple variant where some item is for sale, and where the highest bid wins. We assume the auction is conducted in the usual way, where the price starts at some preset

amount and people place increasing bids until no one wants to bid more than the holder of the currently highest bid. When you enter such an auction, you usually have some (more or less precisely defined) idea of the maximal amount you are willing to pay, and therefore when you will stop bidding. On the other hand, every bidder of course wants to pay as small a price as possible for the item. Indeed, the winner of the auction may hope to pay less than his maximal amount. This will happen if all other bidders stop participating long before the current bid reaches this maximum. For such an auction to work in a fair way, it is obvious that the maximum amount you are willing to pay should be kept private. For instance, if the auctioneer knows your maximum and is working with another bidder, they can force the price to be always just below your maximum and so force you to pay more than if the auction had been honest. Note that the auctioneer has an incentive to do this to increase his own income, which is often a percentage of the price the item is sold for. On the other hand, the result of the auction could in principle be computed, if one was given as input the true maximum value each bidder assigns to the item on sale.

1.1.2 History of Secure MPC

In conclusion secure MPC studies how mutually distrusting users can compute functions of their (private) data via interactive communication in such a way that they do not reveal to each other any more information about their data than can be inferred from learning only the function outputs. The security requirements on an MPC protocol are so stringent that it may seem that it is rarely possible to actually achieve. While the founding works Shamir u. a. (1979); Rabin (1979); Blum (1981); Yao (1982, 1986) were based on computational limitations of the users, seminal papers by Ben-Or, Goldwasser, and Wigderson (Ben-Or u. a., 1988) and Chaum, Crépeau, and Damgård (Chaum u. a., 1988) showed how information theoretically secure computation of any function is possible between parties connected by pairwise, private links as long as only a strict minority may collude in the honest-but-curious model (and a strictly less than one-third minority may collude in the malicious model).

Information-theoretically secure MPC is closely related to the problem of secret sharing (Shamir, 1979) (Verifiable Secret-Sharing in particular) and it would be worthwhile

to look at Appendix A to have a better understanding and appreciate problems in secure MPC. See Beimel (2011) for a comprehensive treatment of secret sharing schemes.

Though information-theoretically secure MPC has been a central primitive of cryptography, relatively less is known about the *efficiency* of such protocols. While there are rich results and techniques for the communication complexity of function computation without security requirements (see for e.g Yao (1979), Kushilevitz (1997), Ma und Ishwar (2013), Prabhakaran und Prabhakaran (2014)), these are mostly not of relevance for the case with security conditions added.

1.2 Prior Work and Contributions

The non-interactive model of secure MPC we study here was proposed by Feige, Kilian, and Naor Feige u. a. (1994) who showed that any function can be securely computed in this model.

For the interactive model, lower bounds for the optimal amount of communication required to securely compute (mainly modular addition) were developed using combinatorial techniques in Franklin und Yung (1992); Chor und Kushilevitz (1993). In a recent work, information theoretic methods were used to develop lower bounds which are tight for several functions of interest Data u. a. (2014); see there for other previous work on lower bounds for communication and randomness.

Our main contribution is the derivation of a lower bound that exploits the structure of the function to be computed and other lower bounds on the entropy of the messages. This lower bound improves upon existing ones, and is seen to be tight in many interesting cases. We also show that in general, there exist protocols outside FKN model that perform strictly better than any protocol in the FKN realm via an example which exploits local randomness to outperform our FKN lowerbound.

CHAPTER 2

MODEL AND PROBLEM DEFINITION

We consider the three-party secure computation model of Feige u. a. (1994) illustrated in Fig. 2.1.

The three parties, called Alice, Bob and Charlie, are connected by pairwise private links as

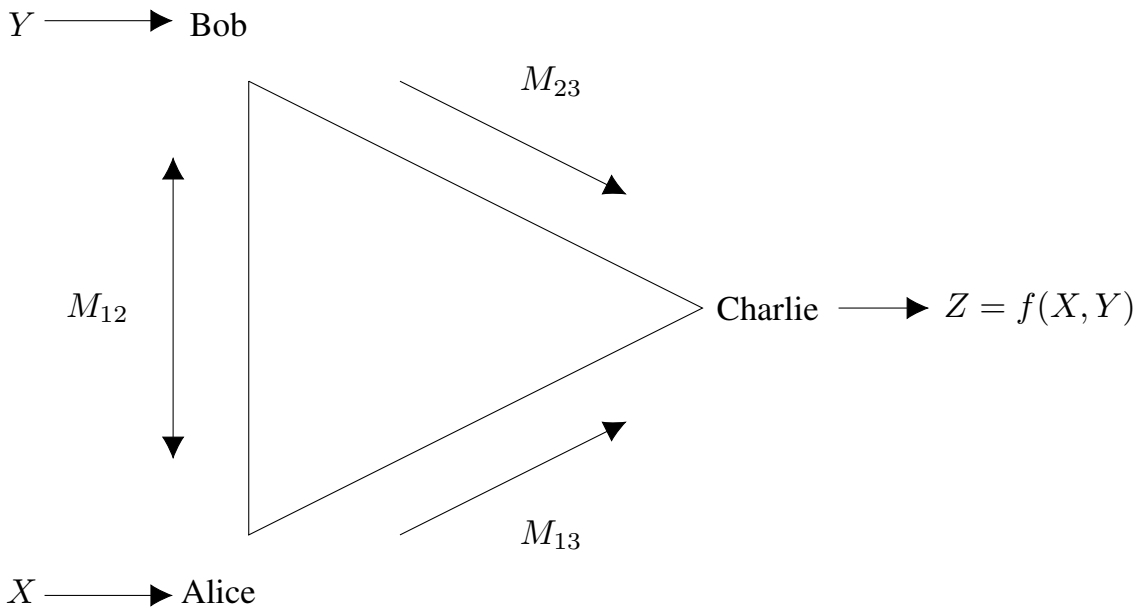

Figure 2.1: Three-party secure computation model.

shown in the figure. Alice and Bob observe input random variables X and Y, respectively, taking values in finite alphabets $\mathcal{X}$ and $\mathcal{Y}$ with joint distribution p_{XY}. The links are noise-free and all transmission are assumed to be instantaneous.

Consider a function $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ taking values in a finite set $\mathcal{Z}$, and let $Z = f(X, Y)$. The goal of our Information theoretic secure computation is for Charlie to compute f *securely* (this is formalized later) and for Alice and Bob to not *learn* anything about the other party's input than what their own input reveals.

2.1 Protocols

In order to accomplish the above task, the participating members follow procedures called *protocols*. While protocols could, in general, involve multiple rounds of communication between the three participants, our model (also called the one-shot model) imposes the following conditions for a protocol to be classified as valid.

1. Alice (or Bob) chooses $M_{12} \in \mathcal{M}_{12}$ according to a distribution $p_{M_{12}}$ and sends it to Bob (or Alice) privately. This can be written as

$$\begin{aligned} M_{12} &- X - Y, Z \\ M_{12} &- Y - X, Z. \end{aligned} \tag{2.1}$$

   M_{12} is not revealed to Charlie.

2. Alice sends $M_{13} \in \mathcal{M}_{13}$, a deterministic function of M_{12} and X, to Charlie. This can be written as

$$H(M_{13}|M_{12}, X) = 0. \tag{2.2}$$

   M_{13} is not revealed to Bob.

3. Bob sends $M_{23} \in \mathcal{M}_{23}$, a deterministic function of M_{12} and his input Y, to Charlie. This can be written as

$$H(M_{23}|M_{12}, Y) = 0. \tag{2.3}$$

   M_{23} is not revealed to Alice.

4. Charlie computes $\hat{Z}$ (his estimate of Z) as a function of M_{13} and M_{23}.

The random variables M_{12}, M_{13}, and M_{23} are referred to as messages, and their alphabets are assumed to be finite. The message M_{13} is a function of M_{12} and X, and the values of M_{13} are denoted as $m_{13} \triangleq m_{13}(m_{12}, x)$. A similar notation $m_{23}(m_{12}, y)$ is used for M_{23}.

We say that a protocol Π is valid in our model if it satisfies conditions 2.1-2.3. For the general model, conditions 2.2 and 2.3 need not hold true and Charlie is allowed to communicate to Alice and Bob. Besides, the number of interactions can be as large as needed.

2.2 Security conditions

Having defined the model, we precisely state the security conditions that need to be satisfied for our information theoretically secure MPC problem:

1. Charlie is to compute Z with zero probability of error,
   i.e.,
   $$H(Z|M_{13}, M_{23}) = 0 \tag{2.4}$$
2. Alice should not learn anything more about Y than what X reveals,
   i.e.,
   $$H(Y|X, M_{13}, M_{12}) = H(Y|X). \tag{2.5}$$
3. Bob should not learn anything more about X than what Y reveals,
   i.e.,
   $$H(X|Y, M_{23}, M_{12}) = H(Y|X). \tag{2.6}$$
4. Charlie should not learn anything more about (X, Y) than what Z reveals,
   i.e.,
   $$H(X, Y|Z, M_{13}, M_{23}) = H(X, Y|Z). \tag{2.7}$$

While our one-shot model seems to be very simplistic and the security conditions 2.4–2.7 seemingly complex (in the sense that the constraints cannot be easily classified as convex, linear or into other common categories), Feige, Kilian, and Naor (Feige u. a., 1994) showed that the above goals can be met in this model for any function. This does not, however, imply that other models of three-party MPC can be ignored. An important point to note in this regard is that the non-interactive and deterministic nature of the protocols in our model completely disregards a huge class of protocols – those that exploit the power of interaction and randomness and which, from a communication complexity point of view, could be more efficient. In fact, we demonstrate that local randomness strictly helps in the case of a particular function.

2.3 Problem definition

Now we are ready to define the optimization problems of interest:

$$\inf_{\Pi} \{H(M_{13})|2.4 - 2.7\} \tag{P.1}$$

$$\inf_{\Pi}\{H(M_{23})|2.4-2.7\} \tag{P.2}$$

$$\inf_{\Pi}\{H(M_{12})|2.4-2.7\} \tag{P.3}$$

In words, given a function f, we are interested in protocols which meet the secure computation goals with the minimum possible communication. We will obtain lower bounds for the entropies $H(M_{12})$, $H(M_{13})$ and $H(M_{23})$, which give lower bounds on the communication needed to accomplish secure computation. We will then demonstrate protocols which meet these lower bounds and, hence, are optimal for some examples of interest.

Lower bounds (see Appendix C) for P.1–P.3 have already been derived in Data u. a. (2014) for the general interactive model. We will use these throughout the paper for deriving our lower bounds and for comparison as well. Note that though these lower bounds are for the interactive model, they apply to our model as well as any valid protocol in our model is also a valid protocol in the general model. In our work, we will mostly be concerned with P.3 as that seems to be the weak point for many functions in Data u. a. (2014).

2.4 Some assumptions

For the rest of this paper, we will assume the following:

- p_{XY} has full support, i.e. every value in the alphabet is taken with a positive probability. Without loss of generality, we will assume that M_{12} has full support.
- No inputs are redundant, i.e. if $f(x,y) = f(x',y)$ for all $y \in \mathcal{Y}$, then $x = x'$, and similarly for the second input to f. Given the full support assumption on p_{XY}, this can be shown to be without loss of generality.

CHAPTER 3

LOWER BOUND ON $H(M_{12})$

3.1 Motivating example: Secure AND

To fix ideas, consider the case where $\mathcal{X} = \mathcal{Y} = \mathcal{Z} = \{0, 1\}$ and $f(X, Y) = XY$ is the AND of two uniformly random bits X and Y. Protocol 1 is a one-shot protocol for secure computation of AND from Feige u. a. (1994).

Protocol 1 : Secure AND

1: Alice randomly and uniformly picks a permutation of $(0, 1, 2)$ - say (α, β, γ) - and sends it to Bob.

2: Alice sends $M_{13} = \alpha$ if $X = 1$ and $M_{13} = \beta$ if $X = 0$ to Charlie, while Bob sends $M_{23} = \alpha$ if $Y = 1$ and $M_{23} = \gamma$ if $Y = 0$.

3: Charlie computes $Z = 1$ if $M_{13} = M_{23}$ or $Z = 0$ otherwise.

It is easy to see that the above protocol satisfies all the requirements of the secure computation of AND. It requires $H(M_{13}) = H(M_{23}) = \log_2 3$ bits on the Alice-Charlie and Bob-Charlie links. These values are known to be optimal even for a more general model where Alice, Bob, and Charlie may interact over multiple rounds Data u. a. (2014). For the Alice-Bob link, the protocol has $H(M_{12}) = \log_2 6$. However, for the interactive model, the lower bound in Data u. a. (2014) is only $1.826 < \log_2 6 \approx 2.585$. One of the contributions of this paper is to show that, for the non-interactive model, $H(M_{12}) \geq \log_2 6$ is, in fact, a lower bound and the protocol is, indeed, optimal for secure AND. Additionally, even for the case of computing the AND of n bits, we show that the repeated use of the Secure AND protocol above is optimal for M_{12}.

Similar ideas are used to obtain lower bounds and prove optimality of protocols for two other computations, namely addition of 0-1 integers and equality testing.

3.2 Lower bound on $|\mathcal{M}_{12}|$ for secure AND

As mentioned before, lower bounds on the entropies of the transcripts on the links in the interactive model were presented in Data u. a. (2014). We will use the bounds on $H(M_{13})$ and $H(M_{23})$ from there (which also apply for our non-interactive model) in combination with the properties of the function f to derive a new lower bound on $H(M_{12})$.

To illustrate the idea involved in the derivation of the bound, we first show that for any one-shot protocol for secure AND, we have $|\mathcal{M}_{12}| \geq 6$. The general lower bound on $H(M_{12})$ is presented later.

Firstly, from Data u. a. (2014), it is known that $H(M_{13}) \geq \log_2 3$ for secure AND, which implies that $|\text{supp}(M_{13})| \geq 3$. Next, we will use the following properties of the AND function, and their implications on the secure AND protocol when the distribution of (X, Y) has full support:

1. $f(1,0) \neq f(1,1)$: For Charlie to compute Z with zero probability of error, it must be the case that supp $((M_{13}, M_{23})|XY = 10)$ and supp $((M_{13}, M_{23})|XY = 11)$ are disjoint.
2. $f(0,0) = f(0,1) = 0$: For Charlie to not differentiate between the inputs (0,0) and (0,1) given $Z = 0$, the supp$((M_{13}, M_{23})|XY = 00)$ and supp$((M_{13}, M_{23})|XY = 01)$ must be identical.

Since

$$[m_{13}(m_{12}, 1),\ m_{23}(m_{12}, 0)] \in \text{supp}\left((M_{13}, M_{23})|XY = 10\right),$$

$$[m_{13}(m_{12}, 1),\ m_{23}(m_{12}, 1)] \in \text{supp}\left((M_{13}, M_{23})|XY = 11\right),$$

and the two support sets above are disjoint, we have that $m_{23}(m_{12}, 0) \neq m_{23}(m_{12}, 1)$ for $m_{12} \in \text{supp}(M_{12})$.

Let $a = m_{13}(m_{12}, 0) \in \mathcal{M}_{13}$ for some $m_{12} \in \mathcal{M}_{12}$, and let $b = m_{23}(m_{12}, 0)$, $b' = m_{23}(m_{12}, 1)$. Note that $b' \neq b$,

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

$$[a,\ b'] \in \text{supp}((M_{13}, M_{23})|XY = 01).$$

Since $\text{supp}((M_{13}, M_{23})|XY = 00)$ and $\text{supp}((M_{13}, M_{23})|XY = 01)$ are identical, we have that

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

as well. Since a appears as $[a, b]$ and $[a, b']$ in $\text{supp}((M_{13}, M_{23})|XY = 00)$, there exists $m'_{12} \in \mathcal{M}_{12}$ such that $a = m_{13}(m'_{12}, 0)$. Thus, corresponding to every message in $\text{supp}(M_{13}|X = 0)$, there are two distinct elements in $\mathcal{M}_{12}$. However, since $f(1, 0) = f(0, 0)$ implies that $\text{supp}(M_{13}|XY = 10) = \text{supp}(M_{13}|XY = 00)$, and (X, Y) has full support, we must have $\text{supp}(M_{13}|X = 0) = \text{supp}(M_{13}|X = 1) = \text{supp}(M_{13})$. This results in the bound

$$|\mathcal{M}_{12}| \geq 2\ |\text{supp}(M_{13})| \geq 6.$$

In the next section, we formally generalize the above arguments to an arbitrary function f. Additionally, we translate the counting argument above into a probabilistic language resulting in bounds on the entropy $H(M_{12})$.

3.3 A general lower bound on $H(M_{12})$

From the previous section, the change or lack of change in $f(x, y)$ when keeping x fixed and altering $y \in \mathcal{Y}$ (or vice versa) plays an important role in the structure of the message sets. Two such useful properties of a one-shot protocol for the secure computation of f are stated in the following lemmas for future reference. Recall that we assume that $p_{X,Y}$ has full support.

Lemma 1. *If $f(x, y) = f(x', y')$, then $(M_{13}, M_{23})|X = x, Y = y$ and $(M_{13}, M_{23})|X = x', Y = y'$ are identically distributed. Further, the marginals $M_{13}|X = x$ and $M_{13}|X = x'$ are identically distributed.*

Proof. Let $z = f(x, y)$. Since $(M_{13}, M_{23}) - Z - (X, Y)$ is a Markov chain, we have

$$\begin{aligned}&\Pr(M_{13} = a, M_{23} = b|Z = z, X = x, Y = y)\\ &= \Pr(M_{13} = a, M_{23} = b|Z = z).\end{aligned}$$

Since $Z = f(X, Y)$, we have $(M_{13}, M_{23}) - (X, Y) - Z$ is a Markov chain, which results in

$$\begin{aligned}&\Pr(M_{13} = a, M_{23} = b | Z = z, X = x, Y = y)\\ &= \Pr(M_{13} = a, M_{23} = b | X = x, Y = y).\end{aligned}$$

Combining, we get

$$\begin{aligned}&\Pr(M_{13} = a, M_{23} = b | Z = z)\\ &= \Pr(M_{13} = a, M_{23} = b | X = x, Y = y).\end{aligned}$$

Since $z = f(x', y')$, we get that

$$\begin{aligned}&\Pr(M_{13} = a, M_{23} = b | Z = z)\\ &= \Pr(M_{13} = a, M_{23} = b | X = x', Y = y')\\ &= \Pr(M_{13} = a, M_{23} = b | X = x, Y = y)\end{aligned}$$

proving the first part of the lemma. Marginalizing over M_{23}, we get that

$$\Pr(M_{13} = a | X = x, Y = y) = \Pr(M_{13} = a | X = x', Y = y').$$

Since $M_{13} - X - Y$ is a Markov chain (since Alice does not learn anything more about Y than what X reveals), we have

$$\Pr(M_{13} = a | X = x, Y = y) = \Pr(M_{13} = a | X = x), \tag{3.1}$$

which completes the proof of the lemma. □

Lemma 2. *Let $x, x' \in \mathcal{X}$ such that $x \neq x'$. Then, for all $m_{12} \in \mathcal{M}_{12}$, $m_{13}(m_{12}, x) \neq m_{13}(m_{12}, x')$. Similarly, $m_{23}(m_{12}, y) \neq m_{23}(m_{12}, y')$ for $y, y' \in \mathcal{Y}$ and $y \neq y'$.*

Proof. Since there are no redundant inputs, there is a $y \in \mathcal{Y}$ such that $f(x, y) \neq f(x,', y)$. If, for any $m_{12} \in \mathcal{M}_{12}$, $m_{13}(m_{12}, x) = m_{13}(m_{12}, x')$, then Charlie will receive the same

message $[m_{13}(m_{12}, x)\ m_{23}(m_{12}, y)]$ for the two different inputs (x, y) and (x', y) when $M_{12} = m_{12}$, which can happen with positive probability, resulting in an error in computation. Hence, for all $m_{12} \in \mathcal{M}_{12}$, $m_{13}(m_{12}, x) \neq m_{13}(m_{12}, x')$. □

The following theorem provides a lower bound on $H(M_{12})$.

Theorem 1. *Let $x \in \mathcal{X}$ and $S \subseteq \mathcal{Y}$ be such that $f(x, y) = f(x, y')$ for $y, y' \in S$, i.e. the elements of S result in the same value of f when $X = x$. Then,*

$$H(M_{12}) \geq H(M_{13}|X = x) + \log_2 |S|. \tag{3.2}$$

Proof. Consider $a = m_{13}(m_{12}, x) \in \mathcal{M}_{13}$ for $m_{12} \in \mathcal{M}_{12}$. Let $S = \{y_1, y_2, \ldots, y_{|S|}\}$ and $b_i = m_{23}(m_{12}, y_i)$. For $i, j \in \{1, \ldots, |S|\}$ and $i \neq j$, by Lemma 2, $b_i \neq b_j$ and

$$[a\ b_i] \in \text{supp}((M_{13}, M_{23})|X = x, Y = y_i).$$

Since $f(x, y_i)$ are equal for all i, we see that

$$[a\ b_i] \in \text{supp}((M_{13}, M_{23})|X = x, Y = y_1)$$

for $i = 1, 2, \ldots, |S|$. So, there exists $m_i \in \mathcal{M}_{12}$ such that $a = m_{13}(m_i, x)$ and $b_i = m_{23}(m_i, y_1)$ for $i = 1, 2, \ldots, |S|$.

By Lemma 1, we have

$$\begin{aligned} &\text{Pr}(M_{13} = a, M_{23} = b_i|X = x, Y = y_i) \\ &= \text{Pr}(M_{13} = a, M_{23} = b_i|X = x, Y = y_1). \end{aligned} \tag{3.3}$$

Using shorthand notation $M_3 = [M_{13}\ M_{23}]$ and $(XY = xy)$ for $(X = x, Y = y)$,

$$
\begin{aligned}
&\Pr(M_{13} = a|X = x) \overset{(a)}{=} \Pr(M_{13} = a|XY = xy_1) \\
&\overset{(b)}{\geq} \sum_{i=1}^{|S|} \Pr(M_{13} = a, M_{23} = b_i|XY = xy_1) \\
&\overset{(c)}{=} \sum_{i=1}^{|S|} \Pr(M_{13} = a, M_{23} = b_i|XY = xy_i) \\
&\overset{(d)}{=} \sum_{i=1}^{|S|} \sum_{m\in\mathcal{M}_{12}} \Pr(M_3 = [a\ b_i], M_{12} = m|XY = xy_i) \\
&\overset{(e)}{=} \sum_{i=1}^{|S|} \sum_{m\in\mathcal{M}_{12}} p_{M_{12}}(m)\Pr(M_3 = [a\ b_i]|XY = xy_i, M_{12} = m) \\
&\overset{(f)}{\geq} |S|\, p_{M_{12}}(m_{12}),
\end{aligned}
$$

where (a) follows from (3.1), (b) follows from marginalization over M_{23} (possibly partial), (c) follows from (3.3), (d) follows from marginalization over M_{12}, (e) follows because M_{12} is independent of (X, Y), and (f) follows because $a = m_{13}(m_{12}, x)$ and $b_i = m_{23}(m_{12}, y_i)$.

Rewriting, we get the upper bound

$$p_{M_{12}}(m_{12}) \leq \frac{\Pr(M_{13} = a|X = x)}{|S|} \tag{3.4}$$

whenever $a = m_{13}(m_{12}, x)$ for $x \in \mathcal{X}$ and $m_{12} \in \mathcal{M}_{12}$.

For $x \in \mathcal{X}$ and $a \in \text{supp}(M_{13}|X = x)$, let $p_{M_{13}|X}(a|x) = \Pr(M_{13} = a|X = x)$ and $\mathcal{M}(a) = \{m \in \mathcal{M}_{12} : m_{13}(m, x) = a\}$. Note that $\mathcal{M}_{12}$ partitions as $\cup_{a\in\text{supp}(M_{13}|X=x)}\mathcal{M}(a)$ and

$$p_{M_{13}|X}(a|x) = p_{M_{13}|XY}(a|xy) = \sum_{m\in\mathcal{M}(a)} p_{M_{12}}(m). \tag{3.5}$$

Now,

$$
\begin{aligned}
H(M_{12}) &= \sum_{m\in\mathcal{M}_{12}} p_{M_{12}}(m)\log_2\left(\frac{1}{p_{M_{12}}(m)}\right)\\
&\overset{(a)}{=} \sum_{a\in\text{supp}(M_{13}|X=x)}\ \sum_{m\in\mathcal{M}(a)} p_{M_{12}}(m)\log_2\left(\frac{1}{p_{M_{12}}(m)}\right)\\
&\overset{(b)}{\geq} \sum_{a\in\text{supp}(M_{13}|X=x)}\ \sum_{m\in\mathcal{M}(a)} p_{M_{12}}(m)\log_2\frac{|S|}{p_{M_{13}|X}(a|x)}\\
&= \log_2|S| - \sum_{a\in\text{supp}(M_{13}|X=x)}\ \sum_{m\in\mathcal{M}(a)} p_{M_{12}}(m)\log_2 p_{M_{13}|X}(a|x)\\
&\overset{(c)}{=} \log_2|S| - \sum_{a\in\text{supp}(M_{13}|X=x)} p_{M_{13}|X}(a|x)\log_2 p_{M_{13}|X}(a|x)\\
&= H(M_{13}|X=x) + \log_2|S|,
\end{aligned}
$$

where (a) follows by the partitioning of $\mathcal{M}_{12}$, (b) from (3.4) and (c) follows from (3.5).

□

Corollary 1. *Let f be such that, for any two inputs $x_1, x_1' \in \mathcal{X}$, there exists $y_1, y_1' \in \mathcal{Y}$ for which $f(x_1, y_1) = f(x_1', y_1')$. For $S \subseteq \mathcal{Y}$ and a fixed $x \in \mathcal{X}$ satisfying $f(x, y) = f(x, y')$ for all $y, y' \in S$, we have*

$$H(M_{12}) \geq H(M_{13}) + \log_2|S|. \tag{3.6}$$

Proof. For f satisfying the condition in the corollary, by Lemma 1, $M_{13}|X = x$ is identically distributed for all $x \in \mathcal{X}$. So, for $a \in \mathcal{M}_{13}$, we have

$$
\begin{aligned}
p_{M_{13}}(a) &= \sum_{x\in\mathcal{X}} \text{Pr}(X=x)\text{Pr}(M_{13}=a|X=x)\\
&= \text{Pr}(M_{13}=a|X=x).
\end{aligned}
$$

This implies that $H(M_{13}) = H(M_{13}|X = x)$ and the proof of the corollary is complete.

□

CHAPTER 4

EXAMPLES

We compute the lower bound developed in the previous section for several interesting functions and prove optimality of protocols in some cases.

4.1 Secure AND

Let $\mathcal{X}, \mathcal{Y}$ be $\{0,1\}^n$, $X = [X_1\ X_2\ \cdots\ X_n]$, $Y = [Y_1\ Y_2\ \cdots\ Y_n]$ with the random variables X and Y having full support over $\mathcal{X} \times \mathcal{Y}$. Let $Z = f(X,Y) = [X_1Y_1\ X_2Y_2\ \cdots\ X_nY_n]$ be the bitwise AND of the inputs.

Consider inputs $x_1, x_1' \in \{0,1\}^n$, and let 0_n denote the length-n, all-zero vector. Now, $f(x_1, 0_n) = f(x_1', 0_n) = 0_n$. Hence, f satisfies the condition of Corollary 1. Using $x = 0_n$ and $S = \{0,1\}^n$, we have

$$H(M_{12}) \geq H(M_{13}) + \log_2 2^n \geq n \log_2 6, \tag{4.1}$$

where $H(M_{13}) \geq n \log_2 3$ from C.1 and $H(M_{23}) \geq n \log_2 3$ from C.2. The above lower bound shows that the protocol of Section 3.1 for Secure AND is optimal for computation of n-bit secure AND.

4.2 Secure 0-1 SUM

Let $\mathcal{X}, \mathcal{Y}$ be $\{0,1\}^n$, $X = [X_1\ X_2\ \cdots\ X_n]$, $Y = [Y_1\ Y_2\ \cdots\ Y_n]$ with the random variables X and Y having full support over $\mathcal{X} \times \mathcal{Y}$. Let $Z = f(X,Y) = [X_1 + Y_1\ X_2 + Y_2\ \cdots\ X_n + Y_n]$ be the integer SUM of the inputs. Note that $\mathcal{Z} = \{0,1,2\}^n$.

Consider inputs $x_1, x_1' \in \{0,1\}^n$, and let 1_n denote the length-n, all-one vector. Now, $f(x_1, 1_n - x_1) = f(x_1', 1_n - x_1') = 1_n$. Hence, f satisfies the condition of Corollary 1. Using $x = 0_n$ and $S = 0_n$, we have

$$H(M_{12}) \geq H(M_{13}) \geq n \log_2 3, \tag{4.2}$$

where $H(M_{13}) \geq n \log_2 3$ from C.1 and $H(M_{23}) \geq n \log_2 3$ from C.2. This is an improvement on the existing bound of $H(M_{12}) \geq 1.5n$ from C.5 proved in Data u. a. (2014) and we prove the optimality of this bound below.

Protocol 2 from Data u. a. (2014) securely computes SUM for $n = 1$:

Protocol 2 : Secure 0-1 SUM

1: Alice randomly and uniformly picks an element from $\{0,1,2\}$ (say α) and sends it to Bob.

2: Alice sends $(X_1 + \alpha) \mod 3$ to Charlie while Bob sends $(Y_1 - \alpha) \mod 3$.

3: Charlie recovers $Z_1 = X_1 + Y_1 \mod 3$.

Repeated use of the above protocol achieves $H(M_{13}) = H(M_{12}) = n \log_2 3$, and is optimal.

4.3 Secure EQ

Let $\mathcal{X} = \mathcal{Y} = \{0, 1, \ldots, Q-1\}$, with the random variables X and Y having full support over $\mathcal{X} \times \mathcal{Y}$. Let $Z = f(X,Y) = \mathbb{1}(X = Y)$ be the indicator function for equality of X and Y. Note that $\mathcal{Z} = \{0,1\}$.

Working out the lower bounds C.3 and C.4, we get $H(M_{13}) \geq \log_2 Q$ and $H(M_{23}) \geq \log_2 Q$.

4.3.1 Lower bound on $H(M_{12})$

Consider inputs $x_1, x_1' \in \{0, 1, \ldots, Q-1\}$. Now, $f(x_1, x_1) = f(x_1', x_1') = 1$. Hence, f satisfies the condition of Corollary 1. Using $x = 0$ and $S = \{1, 2, \ldots, Q-1\}$, we have

$$H(M_{12}) \geq H(M_{13}) + \log_2(Q-1) \geq \log_2(Q(Q-1)), \tag{4.3}$$

where we have used $H(M_{13}) \geq \log_2 Q$.

We remark that the techniques outlined in Data u. a. (2014), namely equation C.5 does not easily yield this particular lower bound (in the interactive model) for $H(M_{12})$. In fact, the best we could obtain (by evaluating bounds on a particular input distribution) was $H(M_{12}) \geq \log(Q) + \frac{Q-1}{Q}\log(Q-1)$, which converges to our lower bound as $Q \to \infty$. Further, since the bounds in Data u. a. (2014) need supremization over input distributions, it is computationally difficult to evaluate RHS of C.5 exactly for all values of Q.

4.3.2 Protocol

Let Π be a set of permutations of the set $[Q] \triangleq \{0, 1, \ldots, Q-1\}$. The set Π is said to be sharply 2-transitive if, for every $i, j, i', j' \in [Q]$ with $i \neq j$ and $i' \neq j'$, there exists exactly one permutation $\pi \in \Pi$ such that $\pi(i) = i'$ and $\pi(j) = j'$ (Grundhöfer und Müller, 2009). Since there are exactly $Q(Q-1)$ pairs (i, j) with $i \neq j$, it follows that $|\Pi| = Q(Q-1)$, if Π is sharply 2-transitive.

For an arbitrary Q, the existence of sharply 2-transitive permutation sets is, in general, not known, and there are instances where sharply 2-transitive permutation sets have been proven to not exist (Grundhöfer und Müller, 2009). However, for the case when Q is a prime power, the set of permutations $\{\alpha x + \beta : \alpha, \beta \in \mathbb{F}_Q, \alpha \neq 0\}$ form a sharply 2-transitive permutation set, where $\mathbb{F}_Q$ is the finite field of order Q (Cameron, 1998).

Suppose Q is such that a sharply 2-transitive permutation set of order Q exists. Let Π be such a set. Protocol 3 describes secure EQ over $\{0, 1, \ldots, Q-1\}$.

Protocol 3 : Secure EQ

1: Alice randomly and uniformly chooses a permutation $\pi \in \Pi$ and sends it to Bob.

2: Alice sends $\pi(x)$ and Bob sends $\pi(y)$ to Charlie.

3: Charlie computes $Z = \mathbb{1}(\pi(x) = \pi(y))$.

The correctness of the above protocol is easy to see. Given that $M_{13} = \pi(x)$, $M_{23} = \pi(y)$ and $\pi(x) \neq \pi(y)$, since Π is sharply 2-transitive, for any pair (x', y') with $x' \neq y'$, there exists exactly one permutation $\pi' \in \Pi$ such that $\pi'(x') = M_{13}$ and $\pi'(y') = M_{23}$. Therefore, the protocol satisfies the security condition for Charlie.

For the above protocol, $H(M_{12}) = \log|\Pi| = \log_2(Q(Q-1))$, $H(M_{13}) = \log_2 Q$, and $H(M_{23}) = \log_2 Q$. This proves the optimality of the protocol.

4.4 Computation of a composite function

Let $X \sim \text{Unif}\{0,1\}$, $Y \sim \text{Unif}\{0,1,2,3\}$ and $Z = f(X,Y)$, where

$$f(X,Y) = \begin{cases} XY & \text{if } Y \in \{0,1\} \\ [(X+Y) \mod 2] + 2 & \text{if } Y \in \{2,3\} \end{cases} \tag{4.4}$$

From Data u. a. (2014), for the interactive model, we have

$$H(M_{13}) \geq \sup_{p_{X'Y'}} (RI(X';Z') + H(X',Y'|Z')),$$

and using the distribution $p_{X'Y'}(0,0) = p_{X'Y'}(0,1) = p_{X'Y'}(1,1) = \frac{1}{3}$, we get $H(M_{13}) \geq \log(3)$. For M_{23}, we have

$$H(M_{23}) \geq \left(\sup_{p_{Y'}} RI(Y';Z')\right) + \left(\sup_{p_{Y''}} H(X,Z''|Y'')\right),$$

which evaluates to $H(M_{23}) \geq \frac{1}{2}\log(20) = 2.16$. For M_{12}, we have

$$H(M_{12}) \geq \sup_{p_{X'}} \left(\sup_{p_{Y'}} RI(Y'; Z') \right) + \left(\sup_{p_{Y''}} RI(X'; Z'') + H(X', Z''|Y'') \right),$$

which evaluates to 2.0.

To obtain a better bound for $H(M_{12})$, we use Corollary 1. Since $f(0,0) = f(1,0)$, the function satisfies the condition in Corollary 1. Now, consider $x = 0$ and $S = \{0,1\} \subseteq \mathcal{Y}$. Since $f(0,0) = f(0,1)$, we get

$$H(M_{12}) \geq H(M_{13}) + \log_2 |S| = \log_2 6,$$

upon using $H(M_{13}) \geq \log_2 3$. This improves on the lower bound of 2 obtained earlier from Data u. a. (2014).

The protocol below is for the secure computation of f.

Protocol 4 : Composite function

1: Alice chooses a permutation of $(0,1,2)$, say (α, β, γ) uniformly at random and sends it to Bob.

2: Alice sends β if $X = 0$ and α if $X = 1$ to Charlie. Bob sends to Charlie $(0,\gamma)$ if $Y = 0$, $(0,\alpha)$ if $Y = 1$, $(1,\alpha)$ if $Y = 2$ and $(1,\beta)$ if $Y = 3$.

3: Charlie computes $Z = \mathbb{1}(M_{23}(2) = M_{13})$ if $M_{23}(1) = 0$ and $Z = \mathbb{1}(M_{23}(2) = M_{13}) + 2$ if $M_{23}(1) = 1$.

Note: $M_{23}(i)$ here refers to the i^{th} symbol that Bob sends to Charlie, for example, if Bob sends $(0,\alpha)$, $M_{23}(1) = 0$ and $M_{23}(2) = \alpha$.

The communication needed for the above protocol is $\log_2 3$ bits on the Alice-Charlie link and $\log_2 6$ bits each on the Alice-Bob and Bob-Charlie link. Note that this is an asymmetric protocol. The Alice-Charlie link and Alice-Bob link are optimal, but the Bob-Charlie link's optimality is still not known. This points to possible improvements in the bounds on $H(M_{13})$ and $H(M_{23})$ in asymmetric cases using properties of the function f.

4.5 A function with an efficient non-FKN protocol

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

$$f(X, Y) = \begin{cases} 2 & \text{if } X = 2 \text{ or } Y = 2 \\ X \oplus Y & \text{else} \end{cases} \tag{4.5}$$

Using C.1 and C.2 we get $H(M_{13}) \geq 2.3137$ and $H(M_{23}) \geq 2.3137$, and using Corollary 1, we get $H(M_{12}) \geq 3.8987$. Consider Protocol 5.

Protocol 5 : Non-FKN protocol

1: Alice chooses a permutation of $(0, 1, 2)$ uniformly at random, say (α, β, γ), and a random bit, say k, and shares it with Bob.

2: Alice sends $\begin{cases} (\alpha, X \oplus k) & \text{if } X \in \{0, 1\} \\ (\beta, k') & \text{else} \end{cases}$.

Bob sends $\begin{cases} (\alpha, Y \oplus k) & \text{if } Y \in \{0, 1\} \\ (\gamma, k'') & \text{else} \end{cases}$,

where k' and k'' are random bits generated from Alice's and Bob's local randomness.

3: Charlie recovers

$$Z = \begin{cases} 2 & \text{if } M_{13}(1) \neq M_{23}(1) \\ M_{13}(2) \oplus M_{23}(2) & \text{else} \end{cases}.$$

Note: $M_{23}(i)$ here refers to the i^{th} symbol that Bob sends to Charlie, for example, if Bob sends $(0, \alpha)$, $M_{23}(1) = 0$ and $M_{23}(2) = \alpha$.

It is easy to see that this protocol requires $\log_2 3 + 1$ bits of communication on the Alice-Charlie and Bob-Charlie links and $\log_2 6 + 1 = 3.58$ bits of communication on the Alice-Bob link. Surely, this is less than our lower bound of 3.89 for the Alice-Bob link, thus pointing to the fact that there may be protocols outside the FKN model of computation which outperform all FKN protocols.

CHAPTER 5

CONCLUSION AND SCOPE FOR FUTURE WORK

In this work, we started out attempting to fix the gap between the communication complexity lower bound for AND computation and the best known upper bound. Interestingly, we end up with more questions than answers. Of course, for a restricted model of computation, we did resolve the question concerning AND computation (and for other functions as well), but the problem remains unsolved for the general interactive model.

The technique used to bound $H(M_{12})$ relied on certain combinatorial structure of the protocols. This indicates the possibility of using advanced combinatorial arguments (like those in communication complexity) in conjunction with information theoretic methods to obtain lower bounds for Secure MPC in general.

For the secure EQ computation, we constructed a protocol based on sharply transitive permutation sets, which are known to exists only for certain orders. Such sets have been proved to *not* exist for some other orders as well, which points to the possibility of more sophisticated protocols for the function. Additionally, from a mathematical perspective, any relation between this information theoretic lower bound for the function and the existence of such sets could be of great interest. For instance, assuming that we get tight lower bounds (either entropy or cardinality bounds) for a general $q - ary$ EQ, can we construct the smallest 2-transitive permutation set of order q?

The last two examples clearly expose the limitations of our lower bounds as well as the one-shot model. The last example specifically raises the question of coming up with tight lower bounds taking local randomness into account. Additionally, the possible advantages of interactive protocols is an interesting topic for future work.

APPENDIX A

SHAMIR'S SECRET SHARING

The Shamir's secret sharing is a scheme (Shamir, 1979) to divide a data D into n pieces – $D_1,\ D_2,\ ..., D_n$ in such a way that

- Knowledge of any k or more pieces of D_i reveals D.
- Knowledge of $k-1$ or fewer pieces of D_i reveals *no* information whatsoever of D, i.e., all values of D are equally likely.

Such a scheme is called a (k, n) threshold scheme.

To motivate the importance of this problem consider the following:
Eleven scientists are working on a secret project. They wish to lock up the documents in a cabinet so that the cabinet can be opened if and only if six or more of the scientists are present. What is the smallest number of locks needed? What is the smallest number of keys to the locks each scientist must carry?
It is not hard to show that the minimal solution uses 462 locks and 252 keys per scientist. These numbers are clearly impractical, and they become exponentially worse when the number of scientists increases.

Shamir's scheme is based on polynomial interpolation. Assume D to be a positive integer. Pick a prime p which is greater than both D and n. Choose $a_1, a_2, ..., a_{k-1}$ randomly from a uniform distribution over $\{0, 1, 2, ..., p-1\}$. Consider the following polynomial

$$q(x) = D + a_1 x + a_2 x^2 + ... + a_{k-1} x^{k-1} \tag{A.1}$$

Now the shares D_i are the evaluations of $q(x)$ at n distinct points, i.e., $D_i = q(x_i)$. Given any subset of k of these D_i values, we can find $q(x)$ by polynomial interpolation and hence $D = q(0)$. But even $k-1$ of these D_i values would not suffice to have any information of D; with $k-1$ values, one can construct only $q'(x)$ which has no information of D.

APPENDIX B

COMPUTING ANY FUNCTION via FKN MODEL

The minimal model of MPC that we study is from Feige u. a. (1994). The following is a protocol to compute any boolean function $f : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$. This extends to k valued functions trivially since each of the $\log k$ output bits represents a boolean function.

Protocol : FKN Protocol

1: Alice sends 2^n random bits $k_0, k_1, ..., k_{2^n-1}$ bits to Bob. Additionally Alice sends j, a n-bit number picked randomly from a uniform distribution in $\{0, 1, ...2^n\}$ to Bob.

2: Alice sends the following string to Charlie: $f(x, j \mod 2^n) \oplus k_{j \mod 2^n}$, $f(x, j+1 \mod 2^n) \oplus k_{j+1 \mod 2^n}$, ..., $f(x, j+2^n-1 \mod 2^n) \oplus k_{j+2^n-1 \mod 2^n}$. This string is nothing but a masked version of all possible output values when $X = x$, and they are cyclically permuted.

3: Bob sends the following to Charlie: k_y and $y - j \mod 2^n$.

4: Charlie computes $f(x, y)$ by picking the $y - j \mod 2^n$-th element from Alice's string, which would be $f(x, y) \oplus k_y$ and XORing it with k_y.

It is easy to see that this preserves the information theoretic security condition of the MPC since Charlie would learn nothing about Alice's and Bob's inputs. The only information he receives is the function value.

APPENDIX C

LOWER BOUNDS ON COMMUNICATION COMPLEXITY FOR THE INTERACTIVE MODEL

Here we state the simplified entropy lower bounds from Data u. a. (2014) without proofs; see there for the proofs and other lower bounds. The following bounds will be used throughout the thesis.

$$H(M_{13}) \geq \sup_{p_{X'Y'}} [I(Y';Z') + H(X',Z'|Y')] \tag{C.1}$$

$$H(M_{23}) \geq \sup_{p_{X'Y'}} [I(X';Z') + H(Y',Z'|X')] \tag{C.2}$$

$$H(M_{13}) \geq \sup_{p_{X'}} \left\{ \left(\sup_{p_{Y'}} I(Y';Z') \right) + H(X') \right\} \tag{C.3}$$

$$H(M_{23}) \geq \sup_{p_{Y'}} \left\{ \left(\sup_{p_{X'}} I(X';Z') \right) + H(Y') \right\} \tag{C.4}$$

$$H(M_{12}) \geq \sup_{p_{X'}} \left\{ \sup_{p_{Y'}} I(Y';Z') + \sup_{p_{Y''}} \{ I(X';Z'') + H(X';Y''|Z'') \} \right\} \tag{C.5}$$

LIST OF PAPERS BASED ON THESIS

1. Sundara Rajan S, Shijin Rajakrishnan, Andrew Thangaraj and Vinod Prabhakaran.: Lower Bounds and Optimal Protocols for Three-Party Secure Computation. *In: 2016 IEEE International Symposium on Information Theory*.

REFERENCES

1. [Beimel 2011] BEIMEL, Amos: Secret-sharing Schemes: A Survey. In: *Proceedings of the Third International Conference on Coding and Cryptology*. Berlin, Heidelberg : Springer-Verlag, 2011 (IWCC'11), S. 11–46. – URL http://dl.acm.org/citation.cfm?id=2017916.2017918. – ISBN 978-3-642-20900-0

2. [Ben-Or u. a. 1988] BEN-OR, Michael ; GOLDWASSER, Shafi ; WIGDERSON, Avi: Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation. In: *Proc. 20th STOC*, ACM, 1988, S. 1–10

3. [Blum 1981] BLUM, Manuel: *Three applications of the oblivious transfer: Part I: Coin flipping by telephone; part II: How to exchange secrets; part III: How to send certified electronic mail*. Technical report, University of California, Berkeley. 1981

4. [Cameron 1998] CAMERON, Peter J.: *Introduction to algebra*. Oxford University Press, 1998

5. [Chaum u. a. 1988] CHAUM, David ; CRÉPEAU, Claude ; DAMGÅRD, Ivan: Multiparty Unconditionally Secure Protocols. In: *Proc. 20th STOC*, ACM, 1988, S. 11–19

6. [Chor und Kushilevitz 1993] CHOR, Benny ; KUSHILEVITZ, Eyal: A Communication-Privacy Tradeoff for Modular Addition. In: *Inf. Process. Lett.* 45 (1993), Nr. 4, S. 205–210

7. [Cramer u. a. 2012] CRAMER, Ronald ; DAMGARD, Ivan ; NIELSEN, Jesper B.: Secure multiparty computation and secret sharing-an information theoretic approach. In: *Book draft* (2012)

8. [Data u. a. 2014] DATA, Deepesh ; PRABHAKARAN, Manoj M. ; PRABHAKARAN, Vinod M.: On the communication complexity of secure computation. In: *Advances in Cryptology–CRYPTO 2014*. Springer, 2014, S. 199–216. – also see http://arxiv.org/abs/1512.07735

9. [Feige u. a. 1994] FEIGE, Uri ; KILIAN, Joe ; NAOR, Moni: A minimal model for secure computation. In: *Proceedings of the twenty-sixth annual ACM symposium on Theory of computing* ACM (Veranst.), 1994, S. 554–563

10. [Franklin und Yung 1992] FRANKLIN, Matthew K. ; YUNG, Moti: Communication Complexity of Secure Computation (Extended Abstract). In: *Proc. 24th STOC*, 1992, S. 699–710

11. [Grundhöfer und Müller 2009] GRUNDHÖFER, Theo ; MÜLLER, Peter: Sharply 2-transitive sets of permutations and groups of affine projectivities. In: *Contributions to Algebra and Geometry* 50 (2009), Nr. 1, S. 143–154

12. [Kushilevitz 1997] KUSHILEVITZ, Eyal: Communication complexity. In: *Advances in Computers* 44 (1997), S. 331–360

13. [Ma und Ishwar 2013] MA, N. ; ISHWAR, P.: The Infinite-Message Limit of Two-Terminal Interactive Source Coding. In: *IEEE Transactions on Information Theory* 59 (2013), July, Nr. 7, S. 4071–4094. – ISSN 0018-9448

14. [Orlandi 2011] ORLANDI, C.: Is multiparty computation any good in practice? In: *2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, May 2011, S. 5848–5851. – ISSN 1520-6149

15. [Prabhakaran und Prabhakaran 2014] PRABHAKARAN, Manoj M. ; PRABHAKARAN, Vinod M.: Tension Bounds for Information Complexity. In: *arXiv preprint arXiv:1408.6285* (2014)

16. [Rabin 1979] RABIN, M. O.: Digitalized Signatures and Public-Key Functions as Intractable as Factorization / Massachusetts Institute of Technology. Januar 1979 (MIT/LCS/TR-212). – Technical Report. – 16 S

17. [Shamir 1979] SHAMIR, Adi: How to share a secret. In: *Communications of the ACM* 22 (1979), Nr. 11, S. 612–613

18. [Shamir u. a. 1979] SHAMIR, Adi ; RIVEST, R. L. ; ADLEMAN, Leonard M.: *Mental poker*. Technical Report LCS/TR-125, Massachusetts Institute of Technology. April 1979

19. [Shannon 1949] SHANNON, C. E.: Communication theory of secrecy systems. In: *The Bell System Technical Journal* 28 (1949), Oct, Nr. 4, S. 656–715. – ISSN 0005-8580

20. [Yao 1982] YAO, Andrew: Protocols for Secure Computation. In: *Proc. 23rd FOCS*, IEEE, 1982, S. 160–164

21. [Yao 1986] YAO, Andrew: How to Generate and Exchange Secrets. In: *Proc. 27th FOCS*, IEEE, 1986, S. 162–167

22. [Yao 1979] YAO, Andrew Chi-Chih: Some Complexity Questions Related to Distributive Computing(Preliminary Report). In: *Proceedings of the Eleventh Annual ACM Symposium on Theory of Computing*. New York, NY, USA : ACM, 1979 (STOC '79), S. 209–213. – URL http://doi.acm.org/10.1145/800135.804414