Lower bounds on communication for multiparty computation
of multiple «AND» instances with secret sharing
Technical Report

Michael Raskin
raskin@mccme.ru
LaBRI, Université de Bordeaux

Abstract

The present report contains a proof of a linear lower bound for a typical three-party secure computation scheme of n independent AND functions. The goal is to prove some linear communication lower bound for a maximally broad definition of «typical».

The article [1] contains various communications lower bounds for unconditionally secure multiparty computation. In particular, it contains a linear lower bound for communication complexity of a regular parallel multiplication protocol using an ideal secret sharing scheme. These conditions mean that the protocol starts with the input being secret-shared with each share of each input field element being a field element, all combinations are used, and the output is shared in the same way as input.

In this report a weaker property of the secret sharing scheme that still allows to prove a linear (w.r.t. the number of multiplications) lower bound on communication is presented. Namely, if we have two (out of three) sides and two options for each party's shares and three possible combinations decode as the same value, the remaining combination should also be a valid pair of shares and reveal the same value.

1 Setting

We assume there are three parties wishing to perform a secure honest-majority parallel computation of «AND» over n pairs of bits. Initially all the inputs are secret-shared in such a way that any two parties can recover the values; after the protocol we want the output to be secret-shared in the same way. We assume that the secret-sharing scheme guarantees perfect information-theoretic privacy.

Definition 1. *A secret sharing scheme is called* ***rectangle-consistent*** *if for every two pairs of possible shares of two parties, $x1, x2$ and $y1, y2$ and for every integer $k \in \{1, \ldots, n\}$ such that (x_1, y_1), (x_1, y_2) and (x_2, y_1) are valid pairs of shares with the same secret bit at position k the pair (x_2, y_2) is also a valid pair of shares and the secret bit at position k is the same.*

Informally speaking, rectangle consistency means that the secret sharing scheme's recovery process never behaves like multiplication.

2 The result

Theorem 1. *Any protocol in the setting using a rectangle-consistent secret sharing scheme has to have $\Omega(n)$ worst-case communication.*

2.1 Proof outline

Let us fix all the randomness and consider the protocol's correctness.

Let us also select two parties (by assumption they will be able to recover the output after the protocol runs) and fix the values of some shares of the input. More specifically, we fix the share of the first input a that the first party gets and the share of the second input b that the second party gets, calling these shares $\overline{a}$ and $\overline{b}$. Perfect privacy means that every possible input is compatible with these shares.

If the protocol has low average communication, there is only a small number of possible protocol logs. Assume there are too few protocol logs. Then there are two pairs of values, a and a' for the first input and b and b' for the second input such that every combination leads to the same protocol if we use $\overline{a}$ and $\overline{b}$ and the corresponding complementary shares. If such pairs of pairs are abundant, for some of them there will be a position k where $a_k \neq a'_k$ and $b_k \neq b'_k$.

Note that if in two situations one party has the same input and at the same time the protocol log is the same, the resulting output share held by this party has to be the same (we have fixed all the random inputs and by assumption nothing seen by the party has changed). That means that the first party's output share depends only on the choice between b and b', and the second party's output share depends only on the choice between a and a'.

But out of the four combinations of shares three correspond to the value 0 in the position k and one corresponds to the value 1. That violates the rectangle consistency property of the secret sharing scheme.

3 Proof

Lemma 1. *For every integer n there is a set S of bit strings of length n such that:*
1. the set S is closed under XOR: $\forall x, y \in S : x \oplus y \in S$;
2. every two nonzero elements of the set S have a common nonzero coordinate: $\forall x, y \in S \setminus \{0\} : x \wedge y \neq 0$;
3. the set S has at least $2^{\frac{n}{6}}$ elements.

Definition 2. *We will call such a set **anti-disjoint**.*

Consider a random set of k uniformly distributed independent random binary vectors $v_1, \ldots, v_k$ with n components each. We need to estimate the probability of the event that the linear span of these vectors satisfies all three conditions.

Let us consider two different nonzero predefined sets of coefficients for two linear combinations, $a_1, \ldots, a_k$ and $b_1, \ldots, b_k$. The random choice of vectors v_i yields two random vectors $v_a = a_1 \times v_1 \oplus \ldots \oplus a_k \times v_k$ and $v_b = b_1 \times v_1 \oplus \ldots \oplus b_k \times v_k$. These two vectors are independent and uniformly distributed. The probability of them having a common nonzero bit at the position j is $\frac{1}{4}$, the probability of not having any common nonzero bits is $\left(\frac{3}{4}\right)^n < 2^{-\frac{n}{3}}$.

The probability that for a random choice of vectors v_j there will be a pair of different nonzero sets of coefficients such that the corresponding linear combinations will not have a common nonzero coordinate can be estimated using a union bound to be at most $(2^k - 1) \times (2^k - 2) \times \left(\frac{3}{4}\right)^n < 2^{2k - \frac{n}{3}}$. If k does not exceed $\frac{n}{6}$, this probability is less than one, therefore it is possible to find a set of basis vectors $v_1, \ldots, v_k$ such that every two distinct nonzero combinations have a common nonzero bit.

Lemma 2. *An $N \times N$ grid coloured using fewer than $N^{\frac{1}{4}}$ colours contains a rectangle with the same colour used for all four vertices.*

Consider such a colouring. Assume there is no rectangle with the same colour used for all corners. Some colour has to be used at least $N^{\frac{7}{4}}$ times. Let's pick $2N^{\frac{1}{4}}$ rows with the most occurrences of the most popular colour. These rows will contain at least $2N$ grid nodes of the most popular colour. Unless there is a rectangle with the same colour in all corners, every two rows have at most one column where these rows both have the most popular colour. Then at most $4N^{\frac{1}{2}}$ columns have more than one point of the most popular colour inside the chosen rows. But there are only N columns, and there are only $2N^{\frac{1}{4}}$ chosen rows. Therefore the total number of the points of the most popular colour in the chosen rows is at most $N + 4N^{\frac{1}{2}} \times 2N^{\frac{1}{4}} = N + 8N^{\frac{3}{4}} < 2N$. This contradiction proves that the assumption was false.

3.1 Proof of the main claim

Assume there is a protocol with the total amount of communication in the worst case less than $\frac{n}{24}$. Fix the first party's share $\overline{a}$ of the input a and the second party's share $\overline{b}$ of the input b. Fix all the randomness used by all the three parties. Consider $N = 2^{\frac{n}{6}}$ inputs from the chosen anti-disjoint set. As there are fewer than $2^{\frac{n}{24}} = N^{\frac{2}{4}}$ possible protocol logs, there are two pairs of inputs, (a, a') and (b, b') such that all the four combinations have the same protocol log if we use complementary shares to $\overline{a}$ and $\overline{b}$. But because the inputs lie in an anti-disjoint set. there is a position where both a versus a' and b versus b' differ. The result bit in this position should be 0 in three out of four combinations and 1 in the remaining case.

Note that the result share of the first party doesn't depend on the choice of the first input, and the result share of the second party doesn't depend on the choice of the second input, because the private inputs and the protocol log are the same. But then if the first two parties recover the result, correctness of the protocol contradicts the rectangle consistency of the secret sharing scheme.

This contradiction proves non-existence of the protocol with sublinear communication.

References

[1] Ivan Damgård, Jesper Buus Nielsen, Antigoni Polychroniadou, Michael Raskin. On the Communication Required for Unconditionally Secure Multiplication. *Advances in Cryptology - CRYPTO Proceedings* 2016, part 2, pp. 459–488.