Lower Bounds for Oblivious Transfer Reductions

Yevgeniy Dodis* Silvio Micali†

March 3, 2001

Abstract

We prove the first *general* and *non-trivial* lower bound for the number of times a 1-out-of-n Oblivious Transfer of strings of length ℓ should be invoked so as to obtain, by an information-theoretically secure reduction, a 1-out-of-N Oblivious Transfer of strings of length L. Our bound is tight in many significant cases and holds even in the honest-but-curious model.

We also prove the first non-trivial lower bound for the number of random bits needed to implement such a reduction whenever the receiver sends no messages to the sender. This bound is also tight in many significant cases.

The novel aspect in deriving these lower bounds is a strong usage of classical information theory.

1 Introduction and Our Results

THE OBLIVIOUS TRANSFER. The *Oblivious Transfer* (OT) is a fundamental primitive in secure protocol design, which has been defined in many different ways and contexts (e.g., [27, 16, 15, 3, 6]) and has found enormously many applications (e.g., [2, 27, 15, 18, 21, 10, 26, 1, 22, 17], to name just a few).

The OT is a protocol typically involving two players, the *sender* and the *receiver*, and several parameters. In the most used form, the $\binom{N}{1}$-OT^L, the sender has N binary secrets of length L, and the receiver gets exactly one of these strings, the one he chooses, but no information about any other secret (even if he cheats), while the sender (even if she cheats) gets no information about the secret learned by the receiver. The most basic and commonly used type of OT corresponds to the sender having just 2 bits (i.e., $N = 2$ and $L = 1$), and is denoted $\binom{2}{1}$-OT.

Also important is the notion of a *weak* Oblivious Transfer[1], a relaxation of the traditional OT. The only difference in a weak $\binom{N}{1}$-OT^L is that a cheating receiver is allowed to obtain partial information about several secrets, but at most L bits of information overall.

REDUCTIONS BETWEEN DIFFERENT OTS. Protocol reductions facilitate protocol design because they enable one to take advantage of implementing cryptographically only a few, carefully chosen, primitives. Information-theoretic reductions are even more attractive, because they guarantee that the security of a complex construction *automatically coincides* with that of the chosen primitive, once the latter is implemented cryptographically.

But to be really useful, reductions must be efficient. In particular, because even the best cryptographic implementation of a chosen primitive may be expensive to run, it is crucial that reductions call such primitives as few times as possible.

Because of the importance of OT, numerous *reductions* from "more complex" to "simpler" OT appear in the literature (e.g. [5, 11, 3, 9, 12]). Particular attention has been devoted to reducing $\binom{N}{1}$-OT^L to $\binom{n}{1}$-OT$^\ell$, where $N \geq n$ and $L \geq \ell$. Typically, these reductions are information-theoretically secure if the simpler OT is assumed to be so secure.

*Department of Computer Science, MIT, Cambridge, MA 02139 (yevgen@theory.lcs.mit.edu).

†Department of Computer Science, MIT, Cambridge, MA 02139 (silvio@tiac.net).

[1] Weak OT is closely related to generalized OT of [3], and is a special case of universal OT of [6].

The best known results about such reductions appeared in the paper of Brassard, Crépeau and Sántha [5] (who extend the results of Brassard, Crépeau and Robert [4]), who showed a simple reduction of $\binom{N}{1}$-OT$^\ell$ to $\binom{2}{1}$-OT$^\ell$ using $(N-1)$ invocations of $\binom{2}{1}$-OT$^\ell$. It is not hard to see (and we show it in Section 4) that this protocol easily generalizes to a reduction from $\binom{N}{1}$-OT$^\ell$ to $\binom{n}{1}$-OT$^\ell$ using $(N-1)/(n-1)$ invocations. Improving upon the ideas of [4], Brassard et. al. also showed an elegant reduction from $\binom{2}{1}$-OT^L to $\binom{2}{1}$-OT (which is the most basic and commonly used type of OT) using $O(L)$ invocations of $\binom{2}{1}$-OT, which again easily generalizes to a reduction from $\binom{N}{1}$-OT^L to $\binom{N}{1}$-OT$^\ell$ with $O(L/\ell)$ invocations. Combining the two results, we get that the best known reduction of $\binom{N}{1}$-OT^L to $\binom{n}{1}$-OT$^\ell$ uses $O(\frac{L}{\ell} \cdot \frac{N-1}{n-1})$ invocations of $\binom{n}{1}$-OT$^\ell$.

We notice that in all the known OT reductions of the above form, the receiver never sends any messages to the sender. An attractive feature of such reductions is that they immediately imply that the sender gets no information about the receiver's index. We call such reductions *one-way*.

OUR QUESTIONS. So far, researchers have been focusing on improving the *upper bounds* of these reductions, that is, the number of times one calls $\binom{n}{1}$-OT$^\ell$ in order to construct $\binom{N}{1}$-OT^L. However, little is known about the corresponding *lower bounds*. Indeed,

> *What is the minimum number of times that the given $\binom{n}{1}$-OT^ℓ must be invoked so as to obtain the desired $\binom{N}{1}$-OT^L?*

Lower bounds were previously addressed in the context of very *specific* reduction techniques, and for very *specific* OTs. For instance, in [5] simple lower bounds are derived for reductions of $\binom{2}{1}$-OT^L to $\binom{2}{1}$-OT^1 that are bound to use *zigzag* functions in a specific way.

Another natural resource of a reduction of $\binom{N}{1}$-OT^L to $\binom{n}{1}$-OT$^\ell$ is the amount of *needed randomness*. That is, an OT protocol is necessary probabilistic, but

> *What is the minimum number of random bits needed in a information-theoretically secure reduction of $\binom{N}{1}$-OT^L to $\binom{n}{1}$-OT^ℓ?*

To the best of our knowledge, no significant results have ever been obtained about this crucial aspect.

OUR RESULTS. In this paper we provide the first *general* lower bounds for such information-theoretic OT reductions, and prove that these bounds are *tight* in significant cases. Namely, we prove that

- In any information-theoretically secure reduction of (even weak!) $\binom{N}{1}$-OT^L to $\binom{n}{1}$-OT$^\ell$, the latter protocol must be invoked at least $\frac{L}{\ell} \cdot \frac{N-1}{n-1}$ times.
- The lower bound is tight for weak $\binom{N}{1}$-OT^L.
- The lower bound is tight for ("strong") $\binom{N}{1}$-OT^L when $L = \ell$.
- The lower bound is always tight up to a small constant factor (at most 5).
- The lower bound holds even in the honest-but-curious model, where both parties are assumed to follow their prescribed protocol.

We also prove the first general lower bound for the amount of randomness needed in a one-way OT reduction. Namely,

- In any one-way reduction of (even weak!) $\binom{N}{1}$-OT^L to $\binom{n}{1}$-OT$^\ell$, the sender must flip at least $\frac{L(N-n)}{n-1}$ coins.
- The lower bound is tight for weak $\binom{N}{1}$-OT^L.
- The lower bound is tight for ("strong") $\binom{N}{1}$-OT^L when $L = \ell$.

We note that, in a one-way reduction, the amount of randomness used by the sender necessarily coincides with the total amount of randomness needed by both parties.

We point out the interesting special case when $n = 2$ and $\ell = 1$, i.e. reducing $\binom{N}{1}$-OT^L to $\binom{2}{1}$-OT, the simplest possible 1-out-2 Oblivious Transfer. We obtain that we need at least $L(N-1)$ invocations of $\binom{2}{1}$-OT and, for a one-way OT reduction, at least $L(N-2)$ random bits. In other words, the number of invocations and the amount of extra randomness are roughly equal to the size of N strings held by the sender, so the sender essentially has to perform an extra 1-out-2 Oblivious Transfer and flip and extra coin for each bit of his information.

LOWER BOUNDS VIA INFORMATION THEORY. No general lower bound for OT reduction would be provable without very precisely and generally defining what such a reduction is. Fortunately, one such definition was successfully given by Brassard, Crépeau, and Sántha [5] based on information theory, and in particular the notion of *mutual information*. This framework is very useful since it allows one to define precisely such intuitive (but hard to capture formally) notions as "learn at most k bits of information" or "learn no information other than ...".

We point out, however, that information theory is much more useful than merely defining the problem. Indeed, we shall demonstrate that its powerful machinery is essential in *solving* our problem, for example, in proving our $\frac{L}{\ell} \cdot \frac{N-1}{n-1}$ lower bound on the number of invocations. Only the trivial bound of $\frac{L}{\ell}$ appears to be provable without information theory. But getting the additional $\frac{N-1}{n-1}$ factor in the lower bound (which is essential when $L = \ell$) requires explicit or implicit use of information theory.

We believe and hope that information theory will prove useful for other types of lower bounds in protocol problems.

ORGANIZATION. In Section 2 we define the information-theoretic notions that we will use, as well as the formal definitions of Oblivious Transfer and Oblivious Transfer reductions. Section 3 is devoted to proving the lower bounds on the number of invocations and the number of random coins needed. Section 4 will show the matching upper bounds. Finally, Section 5 will have the concluding remarks.

2 Preliminaries

2.1 Information Theory Background

Let X, Y, Z by random variables over domains $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$. Let us denote by $P_X(x)$, $P_{X|Z}(x|z)$, $P_{X,Y}(x,y)$ the probability distribution of X, conditional probability distribution of X given Z, and joint distribution of X and Y respectively.

Definition 1

- *The* entropy $\mathbf{H}(X) = -\sum_x P_X(x) \log_2 P_X(x)$.

  The entropy of a random variable X tells how many truly random bits one can extract from X, i.e. how much "uncertainty" is in X.

- *The* conditional entropy $\mathbf{H}(X|Z)$ *is the average over z of the entropy of the variable X_z distributed according to $P_{X|Z}(x|z)$ (denoted $\mathbf{H}(X|Z=z)$), i.e.*

$$\mathbf{H}(X|Z) = \sum_z P_Z(z)\mathbf{H}(X|Z=z) = -\sum_z P_Z(z) \sum_x P_{X|Z}(x|z) \log_2 P_{X|Z}(x|z)$$

  $\mathbf{H}(X|Z)$ *measures how much uncertainty X still has when one knows Z.*

- *The* joint entropy *of X and Y is the entropy of the joint variable (X,Y), i.e.*

$$\mathbf{H}(X,Y) = -\sum_{x,y} P_{X,Y}(x,y) \log_2 P_{X,Y}(x,y)$$

- *The* mutual information *between X and Y is* $\mathbf{I}(X;Y) = \mathbf{H}(X) - \mathbf{H}(X|Y)$.
- *The* mutual information between X and Y given Z *is* $\mathbf{I}(X;Y|Z) = \mathbf{H}(X|Z) - \mathbf{H}(X|(Y,Z))$.

  The mutual information between X and Y (given Z) tells how much "common information" is between X and Y (given Z), i.e. by how much the uncertainty of X (given Z) decreases after one learns Y.

The following easily verified lemma summarizes some of the properties we will need (for the proof and further reference in information theory, see [8]).

Lemma 1

1. $\mathbf{H}(X,Y) = \mathbf{H}(X) + \mathbf{H}(Y|X) = \mathbf{H}(Y) + \mathbf{H}(X|Y)$.
2. $\mathbf{I}(X;Y) = \mathbf{I}(Y;X) = \mathbf{H}(Y) - \mathbf{H}(Y|X) = \mathbf{H}(X) - \mathbf{H}(X|Y) = \mathbf{H}(X) + \mathbf{H}(Y) - \mathbf{H}(X,Y)$.
3. $\mathbf{I}(X,Z;Y) = \mathbf{I}(X;Y) + \mathbf{I}(Z;Y|X)$.
4. $\mathbf{H}(X|Y) = 0$ *iff X is a deterministic function of Y.*
5. $\mathbf{H}(X|Y) \leq \mathbf{H}(X)$ *with equality iff X and Y are independent.*
   (Thus, $\mathbf{I}(X;Y) \geq 0$ with equality iff X and Y are independent.)
6. $\mathbf{I}(X;Y) \leq \mathbf{H}(X) \leq \log_2 |\mathcal{X}|$.
7. $\mathbf{I}(X;Y) \leq \mathbf{I}(X;Y|Z) + \mathbf{H}(Z)$.
8. $\mathbf{H}(U_n) = n$, *where U_n is the uniform distribution over n-bit strings.*

Items 1. and 3. are called "the chain rule" of entropy and mutual information, respectively. Item 2. shows that the mutual information is symmetric in X and Y. Item 4. says that X has no uncertainty given Y if and only if it can be determined from Y. Item 5. says that conditioning can only reduce the uncertaintly, so extra-information "never hurts". In particular, the mutual information is always non-negative and is zero only if X and Y are independent. Item 6. says that one cannot have more common information between X and Y than there is uncertainty in X, which in turn is no more than $\log |\mathcal{X}|$. In fact, equality can be achieved only by the uniform distribution on $\mathcal{X}$. In particular, the uniform distribution over n-bit strings has n bits of uncertainty, as expected (item 8.). Finally, Item 7. says that extra-information Z can decrease the mutual information between X and Y by at most the amount of uncertainty that Z has (and can reveal).

2.2 Information-Theoretically Secure OT Reductions

We can now formally define (1) protocols with an ideal $\binom{n}{1}$-OT$^\ell$ and (2) information-theoretically secure reduction of $\binom{N}{1}$-OT^L to $\binom{n}{1}$-OT$^\ell$. Despite the difference in presentation, the following definition is a *simplification* of that of [5]. For instance, we simplify it by ignoring the additional condition of *awareness* that is not going to affect our lower bound in any way. Another difference is that [5] define $\binom{N}{1}$-OT^L "by itself", rather than in the context of having a "built-in" black-box for $\binom{n}{1}$-OT$^\ell$. While seemingly more elegant, this definition is vacuous on its own, since no two-party protocol can actually implement Oblivious Transfer with information-theoretic security.

Interactive Turing Machines (ITMs). A pair of interactive Turing machines (ITMs) is a pair of two probabilistic Turing machines, each of which has a special communication tape. The joint computation proceeds in phases. In each phase only one machine is active. It can perform an arbitrary computation, at the end of which it sends some string s to the other machine by placing s on its communication tape. In the next round the other machine becomes active, and receives the string s by having it written on its communication tape. At the end of computation both machines compute their local outputs. (See [20] for a more detailed exposition.)

Protocols with ideal $\binom{n}{1}$-OT$^\ell$. Let us denote by a *n-sender* a probabilistic ITM having n special registers, and by a *n-receiver* is probabilistic ITM having a single special register. Let A be a n-sender and

B a n-receiver. We say that (A, B) is a *protocol with ideal* $\binom{n}{1}$-OT^{ℓ} if, letting a be a private input for A and b be a private input for B, the computation of (A, B) proceeds as that of pair of ITMs, except that it consists of three (rather than the usual two) types of rounds: sender-rounds, receiver-rounds and OT-rounds, where by convention the first round always is a sender-round and the last is a receiver-round. In a sender-round, only A is active, and it sends a message to B (that will become an input to B at the start of the next receiver-round). In a receiver-round, only B is active and, except for the last round, it sends a message to A (this message will become an input to A at the start of the next sender-round). In an OT round,

(1) A places for each $j \in [n]$ an ℓ-bit string σ_j in its j-th special register, and

(2) B places an integer $i \in [n]$ in its special register, and

(3) σ_i will become a distinguished input to B at the start of the next receiver-round. A will obtain no information about i.

At the end of any execution of (A, B), B computes a distinguished string called B's *output*.

MESSAGES AND VIEWS. Let (A, B) be a protocol with ideal $\binom{n}{1}$-OT^{ℓ}. Then, in an execution of (A, B), we refer to the messages that A sends in a sender-round as A's *ordinary messages*, and to the strings that A writes in its special registers in an OT-round as A's *potential OT messages*. For each OT-round, only one of the n potential messages will be received by B, and we shall refer to all such received messages as B's *actual OT messages*. Recalling that both A and B are probabilistic, in a random execution of (A, B) where the private input of A is a and the private input of B is b, let us denote by $\mathrm{VIEW}_A[A(a), B(b)]$ the random variable consisting of

(1) a, (2) A's coin tosses, and (3) the ordinary messages received by A;

and let us denote by $\mathrm{VIEW}_B[A(a), B(b)]$ the random variable consisting of

(1) b, (2) B's coin tosses, and (3) all messages (both the ordinary and the actual OT ones) received by B.

REDUCTION OF $\binom{N}{1}$-OT^{L} TO $\binom{n}{1}$-OT^{ℓ}. Denote by $\mathcal{W}$ the set of all N-long sequences of L-bit stings and, given $w \in \mathcal{W}$, let w_i be the i-th string of w. Denote by W the random variable that selects an element of $\mathcal{W}$ with uniform probability; by I the random variable selecting an integer in $[N]$ with uniform probability; and let A be an n-sender and B be an n-receiver. We say that (A, B) is an *information-theoretically secure* reduction of $\binom{N}{1}$-OT^{L} to $\binom{n}{1}$-OT^{ℓ} if the following three properties are satisfied:

(P1) (Correctness) $\forall w \in \mathcal{W}$ and $\forall i \in [N]$, and $\forall$ execution of (A, B) where A's private input is w and B's private input is i,

$$B\text{'s output is } w_i;$$

(P2) (Receiver Privacy) $\forall$ sender A' and $\forall$ string a',

$$\mathbf{I}(\mathrm{VIEW}_{A'}[A'(a'), B(I)] \ ; \ I) = 0; \tag{1}$$

(P3) (Sender Privacy) $\forall$ receiver B' and string b', $\exists$ a random variable $\tilde{I} \in [N]$ *independent* of W s.t.

$$\mathbf{I}(W \ ; \ \mathrm{VIEW}_{B'}[A(W), B'(b')] \mid W_{\tilde{I}}) = 0. \tag{2}$$

In the context of a reduction of $\binom{N}{1}$-OT^{L} to $\binom{n}{1}$-OT^{ℓ}, we shall sometimes say that we are given $\binom{n}{1}$-OT^{ℓ} as a black-box.

The Correctness Property states that when A and B are honest, B will always obtain the string he wants. The Receiver Privacy Property states that no malicious sender A' can learn any information about the index of the honest receiver B. Finally, the Sender Privacy Property states that a malicious receiver B' can learn information about *at most one* of N strings of the sender A. Moreover, the index $\tilde{I}$ of this single string cannot depend on W (e.g. we don't want B' to learn the first string in W that starts with 10). In other words, both A and B do not gain anything by not following the protocol.

REDUCTION OF WEAK $\binom{N}{1}$-OT^L TO $\binom{n}{1}$-OT$^\ell$. We call (A, B) an *information-theoretically secure* reduction of weak $\binom{N}{1}$-OT^L to $\binom{n}{1}$-OT$^\ell$ if all the properties of the reduction of $\binom{N}{1}$-OT^L to $\binom{n}{1}$-OT$^\ell$ hold except (Sender Privacy) is relaxed to the following:

(P3′) (Weak Sender Privacy) $\forall$ receiver B' and string b'

$$\mathbf{I}(W \ ; \ \mathrm{VIEW}_{B'}[A(W), B'(b')]) \leq L. \tag{3}$$

This property says that we allow a malicious receiver B' to obtain partial information about possibly *several* strings, provided he learns *no more than L bits* of information overall. To emphasize the difference, we will sometimes refer to the (regular) reduction between $\binom{N}{1}$-OT^L and $\binom{n}{1}$-OT$^\ell$ as reducing *strong* $\binom{N}{1}$-OT^L to $\binom{n}{1}$-OT$^\ell$. To justify this terminology, we show

Lemma 2 *If (A, B) is a reduction of (strong) $\binom{N}{1}$-OT^L to $\binom{n}{1}$-OT^ℓ, then it is a reduction of weak $\binom{N}{1}$-OT^L to $\binom{n}{1}$-OT^ℓ.*

Proof: By Lemma 1 (equations 7 and 6) and Sender Privacy (P3)

$$\begin{aligned} \mathbf{I}(W; \mathrm{VIEW}_{B'}[A(W), B'(b')]) &\leq \mathbf{I}(W; \mathrm{VIEW}_{B'}[A(W), B'(b')] \mid W_{\bar{I}}) + \mathbf{H}(W_{\bar{I}}) \\ &= \mathbf{H}(W_{\bar{I}}) \leq |W_{\bar{I}}| = L \end{aligned}$$

■

3 Lower Bounds

To simplify our notation, we do not worry about "floors" and "ceilings" in the rest of the chapter, assuming that $(N-1)$ is divisible by $(n-1)$ and that L is divisible by ℓ (handling the the general case presents no significant difficulties). We will also refer to the sender as Alice and to the receiver as Bob.

Throughout, let α be the number of OT-rounds (invocations of $\binom{n}{1}$-OT$^\ell$) needed to reduce (weak) $\binom{N}{1}$-OT^L to $\binom{n}{1}$-OT$^\ell$. Since we concentrate on the worst possible number of OT-rounds, we can assume w.l.o.g. that α is a fixed number and that the sender and receiver always perform exactly α OT-steps. We start with a sharp lower bound on α, and then show a bound on the amount of randomness in a one-way reduction.

3.1 Lower Bound on the Number of Invocations

Let us first give the *informal* intuition behind out lower bound: $\alpha \geq \frac{L}{\ell} \cdot \frac{N-1}{n-1}$. We know by the (weak) sender privacy condition that Bob can learn at most L (out of total NL) bits of information about W. However, if in each of the OT rounds Bob was somehow able to obtain *all* n strings that Alice put as her local inputs to this OT round (rather than getting only one of them), Bob should be able to learn all (NL bits) of W. Indeed, if Bob could not cannot learn some W_i with certainty, Alice will know that Bob's index is not i (if it was i, honest Bob should be able to get W_i with probability 1 by the correctness property). But this would contradict the receiver privacy condition as Alice learns some information about Bob's index. Hence, $\alpha n\ell - n\ell = \alpha\ell(n-1)$ bits that Bob did *not* get from the OT rounds, "contain information" about the remaining at least $NL - L = L(N-1)$ bits of W that Bob did not learn. The bound follows. Let us now turn this intuition into a formal proof.

Theorem 1 *Any information-theoretically secure reduction of* weak[2] $\binom{N}{1}$-OT^L *to* $\binom{n}{1}$-OT^ℓ *must have*

$$\alpha \geq \frac{L}{\ell} \cdot \frac{N-1}{n-1} \tag{4}$$

[2]Since we are proving a lower bound, it clearly applies to (strong) $\binom{N}{1}$-OT^L as well.

Proof: Let P, $P = (Alice, Bob)$, be an information-theoretically secure reduction of $\binom{N}{1}$-OT^L to $\binom{n}{1}$-OT$^\ell$ that uses α invocations to $\binom{n}{1}$-OT$^\ell$. First, we need the following simple lemma.

Local Lemma: For any input $w = w_1, \ldots, w_N$, any random tape R_A for Alice, any distinct $i, i' \in [N]$ and any random tape tape R'_B for Bob, there exists a tape R_B for Bob such that the sequence of messages, M, received by $Alice(w, R_A)$ from $Bob(i', R'_B)$ coincides with the sequence of messages that $Alice(w, R_A)$ receives from $Bob(i, R_B)$.

Proof: Assume that R_B does not exist. Then, executing with $Bob(i', R'_B)$, we get that $Alice(w, R_A)$ will determine for sure that Bob's index is not i. Thus, when Bob's index is i', with non-zero probability over Bob's random string, $Alice(w, R_A)$ would obtain information about Bob's index (that it is not i), contradicting the receiver privacy condition. □

To derive our lower bound for α, we define the following two notions: that of a special execution of P and that of a pseudo-execution of P.

SPECIAL EXECUTION. A *special execution of* P is an execution of P in which Alice's input is a sequence of N randomly selected strings of length L, Alice's tape consists of randomly and independently selected bits, Bob's index is 1, and Bob's tape is the all-zero string, $\vec{0}$. In other words, we fix the behavior of Bob by fixing his index and the random string. With respect to a special execution of P, define the following random variables:

- W — Alice's N L-bit strings, $W = W_1, \ldots, W_N$;
- R — Alice's random tape;
- M_s — the ordinary messages sent by sender Alice;
- M_r — the ordinary messages sent by receiver Bob;
- V — Alice's potential messages (an $\alpha n\ell$-bit string, that is, for each of the α invocations of $\binom{n}{1}$-OT$^\ell$, the n ℓ-bit strings that are Alice's local inputs in the invocation).
- V_r — the actual messages received by Bob in the OT-rounds, (an $\alpha\ell$-bit string, that is, for each of the α invocations of $\binom{n}{1}$-OT$^\ell$, the ℓ-bit string that Bob received depending on his local index during that invocation).

PSEUDO-EXECUTION. Let $\bar{M}_s$ be a sequence of messages, let $\bar{V}$ be a sequence of α sequences of n strings of length ℓ each, let $\bar{i}$ be an index in $[N]$, and let $\bar{R}_B$ be a bit-sequence. A *pseudo-execution of* P with inputs $\bar{M}_s$, $\bar{V}$, $\bar{i}$, and $\bar{R}_B$, denoted by $\bar{P}(\bar{M}_s, \bar{V}, \bar{i}, \bar{R}_B)$, is the process of running Bob with index $\bar{i}$ and coin tosses $\bar{R}_B$, letting the k-th message from the sender be the k-th string of $\bar{M}_s$, and by letting the sender's input to the j-th invocation of $\binom{n}{1}$-OT$^\ell$ to be the j-th n-tuple of ℓ-bit strings in $\bar{V}$. In other words, we pretend to be Alice and see what Bob will do in this situation on some particular index and random string.

Our lower bound for α immediately follows from the following two claims.

Local Claim 1: $\mathbf{I}((V, M_s)\ ;\ W) = NL$.

Proof: By the definition of mutual information, we have

$$\mathbf{I}((V, M_s)\ ;\ W) = \mathbf{H}(W) - \mathbf{H}(W \mid (V, M_s)).$$

Because W is randomly selected, $\mathbf{H}(W) = NL$. Therefore, to establish our claim we must prove that $\mathbf{H}(W \mid (V, M_s)) = 0$. We do that by showing that W is computable from V and M_s by means of the following algorithm.

1. Run $\bar{P}(V, M_s, 1, \vec{0})$ and let M_r be the resulting "ordinary messages sent by Bob".

   (*Comment:* Bob's view and Bob's messages sent in this pseudo-execution are distributed exactly as in a special execution.)

2. For $i = 1 \ldots N$ compute W_i as follows:

- Find a string R_i such that, when executing $\bar{P}(V, M_s, i, R_i)$, the sequence of messages sent by Bob equals M_r.

  (*Comment:* The *existence* of at least one such R_i follows from the Local Lemma with $i' = 1$, $R'_B = \vec{0}$, $w = W$ and $R_A = R$. Further notice that, because M_r, W and R totally determine Alice's behavior, the messages and "potential" messages that $Alice(W, R)$ sends to $Bob(1, \vec{0})$ and to $Bob(i, R_i)$ are exactly V and M_s in both cases. Hence, *any* R_i that produces M_r in the pseudo-execution $\bar{P}(V, M_s, i, R_i)$, implies that $Alice(W, R)$ would produce messages M_s and "potential" messages V when communicating with $Bob(i, R_i)$.)
- Let W_i be *Bob*'s output in $\bar{P}(V, M_s, i, R_i)$.

  (*Comment:* By the correctness property of our reduction, $Bob(i, R_i)$ would correctly output W_i when talking to $Alice(W, R)$. And as we noticed, $Alice(W, R)$ would produce M_s and V when communicating with $Bob(i, R_i)$, so running pseudo-execution $\bar{P}(V, M_s, i, R_i)$ indeed makes Bob to produce the correct W_i).

□

Local Claim 2: $\mathbf{I}((V, M_s)\ ;\ W) \leq L + \alpha\ell(n-1)$.

Proof: By Lemma 1 (equation 3), we have

$$\mathbf{I}((V, M_s)\ ;\ W) = \mathbf{I}((V_r, M_s)\ ;\ W) + \mathbf{I}((V \backslash V_r)\ ;\ W \mid (V_r, M_s)).$$

Now, because P implements *weak* $\binom{N}{1}$-OT^L, and because (V_r, M_s) consists of Bob's view in a (special) execution of P, we have by (P3′) that $\mathbf{I}((V_r, M_s)\ ;\ W) \leq L$. Also, by Lemma 1 (equations 5 and 6),

$$\mathbf{I}((V \backslash V_r)\ ;\ W \mid (V_r, M_s)) \leq |V \backslash V_r| = \alpha\ell(n-1).$$

The claim follows. □

By combining Local Claims 1 and 2, we have $NL \leq L + \alpha\ell(n-1)$, from which the desired lower bound for α immediately follows.

■

Notice from the proof of Theorem 1 that the bound on the number of invocations of $\binom{n}{1}$-OT$^\ell$ holds even in the *honest-but-curious* model, i.e. even if we want the sender and the receiver privacy to hold *only* for honest Alice and Bob. Indeed, all the arguments within the proof had Alice and Bob follow the prescribed protocol. Thus, even if we trust the participants to follow the protocol, we need at least this many invocations to ensure privacy.

We also remark that Maurer [23] isolated the properties of Oblivious Transfer used in establishing Theorem 1 and defined slightly more general forms of $\binom{N}{1}$-OT^L and $\binom{n}{1}$-OT$^\ell$ for which the same proof goes through. These generalizations do not seem to be very natural, but make the proof slightly clearer by distilling the essential properties of the OT that we use.

3.2 Lower Bound on the Number of Random Bits

Let us now prove the lower bound on the number of random bits needed by the sender in a one-way reduction.

Theorem 2 *In any information-theoretic one-way reduction of* **weak**[3] $\binom{N}{1}$*-OT*^{L} *to* $\binom{n}{1}$*-OT*$^\ell$ *the sender must flip at least* $\frac{L(N-n)}{n-1}$ *random coins.*

Proof: Let P, $P = (Alice, Bob)$, be an information-theoretically secure one-way reduction from weak $\binom{N}{1}$-OT^L to $\binom{n}{1}$-OT$^\ell$. As before, let W be the random input of Alice, R be her random tape, M_s be her ordinary messages sent to Bob and V be her "potential" messages. We notice that since the reduction is one-way, the distribution of V and M_s does not depend on Bob's index and his random string. Let V_j, $j = 1 \ldots n$, be an α-tuple consisting of string number j taken from each of the α invocations of $\binom{n}{1}$-OT$^\ell$. We see that V is the disjoint union of $V_1, \ldots, V_n$.

[3] Again, same result applies to (strong) $\binom{N}{1}$-OT^L as well.

As before, we proceed by expanding the mutual information between W and (V, M_s) in two different ways.

$$\mathbf{I}((V, M_s); W) = \mathbf{H}(W) - \mathbf{H}(W \mid (V, M_s)) = NL - 0 = NL \tag{5}$$

Here we used the fact that W is determined from V and M_s. Indeed, since V and M_s do not depend on Bob's input or random string, Alice should make sure that honest Bob can retrieve any W_i with probability 1 (if his input is i).

On the other hand, it is a possible behavior for a (malicious) Bob to read string number j in all the OT-rounds, i.e. to obtain V_j. By the weak sender privacy condition, $\mathbf{I}((V_j, M_s); W) \leq L$, and, therefore, for any $j \in [n]$ we have (using Lemma 1, equations 5 and 6)

$$\mathbf{I}((V, M_s); W) = \mathbf{I}((V_j, M_s); W) + \mathbf{I}(V \backslash V_j; W \mid (V_j, M_s)) \leq L + \mathbf{H}(V \backslash V_j \mid V_j)$$

Combining this with Equation (5), we get

$$\mathbf{H}(V \backslash V_j \mid V_j) \geq L(N-1), \qquad \forall j \in [n] \tag{6}$$

Since V is a disjoint union of V_j's, we get from the above equation (for $j = n$) and Lemma 1 (equations 1 and 5) that $L(N-1) \leq \mathbf{H}(V \backslash V_n \mid V_n) \leq \sum_{j=1}^{n-1} \mathbf{H}(V_j \mid V_n)$. Hence, there is an index $j \in [n-1]$ s.t. $\mathbf{H}(V_j) \geq \mathbf{H}(V_j \mid V_n) \geq \frac{L(N-1)}{n-1}$. W.l.o.g. assume $j = 1$, i.e. $\mathbf{H}(V_1) \geq \frac{L(N-1)}{n-1}$. Since for a fixed W, the only randomness of V came from R, we have by Equation (6) and Lemma 1 (equation 1)

$$\begin{aligned} |R| &\geq \mathbf{H}(V \mid W) = \mathbf{H}(V, W) - \mathbf{H}(W) = \mathbf{H}(V_1) + \mathbf{H}(V \backslash V_1 \mid V_1) - NL \\ &\geq \frac{L(N-1)}{n-1} + L(N-1) - LN = \frac{L(N-n)}{n-1} \end{aligned}$$

Here $\mathbf{H}(V, W) = \mathbf{H}(V)$ as W is a function of V, and then we use (6) for $j = 1$ and our assumption on $\mathbf{H}(V_1)$. This completes the lower bound proof. ∎

We notice that unlike the lower bound proof on the number of invocations, the proof above does not hold in the honest-but-curious model. Namely, it uses the fact that the sender Alice should be protected even against the *malicious* receiver Bob. This is not surprising since no randomness is needed in the honest-but-curious model. For example, to reduce $\binom{N}{1}$-OT^L to $\binom{n}{1}$-OT$^\ell$ we could use $NL/(n-1)\ell$ invocations of $\binom{n}{1}$-OT$^\ell$, where each of these invocations will have a zero-string in the first position, and the remaining positions are filled with NL "data"-bits greedily split into ℓ-chunks (where L/ℓ chucks from each w_i are in different OT's). We simply trust Bob to read L/ℓ chucks of w_i, and to read the all-zero string from the remaining OT's.

4 Upper Bounds

Though our main contribution is establishing the lower bounds in Section 3, we now touch upon the upper bounds to demonstrate the tightness of Theorems 1 and 2. This is done by means of a *single* one-way reduction of weak $\binom{N}{1}$-OT^L to $\binom{n}{1}$-OT$^\ell$ that *simultaneously* achieves both the lower bounds for the number of invocations of $\binom{n}{1}$-OT$^\ell$ and the number of random bits needed by the sender. This protocol is a simple generalization of the one given by Brassard, Crépeau and Sántha [5] and Brassard, Crépeau and Robert [4] for the case $L = \ell$, $n = 2$. For completeness purposes, we also include the proof that this protocol works. Though a similar proof could be derived from [5], the one included here is more direct because our definition of a reduction is slightly simpler.[4] Note that the same protocol also proves that our lower bounds are tight for reduction of (strong) $\binom{N}{1}$-OT$^\ell$ to $\binom{n}{1}$-OT$^\ell$ (i.e., $L = \ell$). At the end of this section we will also show that the bound on the number of invocations is tight up to a small constant factor even when $L > \ell$, by slightly generalizing another protocol of [5, 4].

[4] You might notice, we embed the security of $\binom{n}{1}$-OT$^\ell$ into the definition of our reduction. Without doing so, one would have to argue about "nested mutual information".

OT #	Zero-String	One-String
1	w_1	x_1
2	$w_2 \oplus x_1$	$x_2 \oplus x_1$
3	$w_3 \oplus x_2$	$x_3 \oplus x_2$
$\ldots$	$\ldots$	$\ldots$
$N-2$	$w_{N-2} \oplus x_{N-3}$	$x_{N-2} \oplus x_{N-3}$
$N-1$	$w_{N-1} \oplus x_{N-2}$	$w_N \oplus x_{N-2}$

Figure 1: Special case of using $\binom{2}{1}$-OT$^\ell$, i.e. $n = 2$.

4.1 Reducing weak $\binom{N}{1}$-OT^L to $\binom{n}{1}$-OT$^\ell$

Theorem 3 *There exists a one-way information-theoretically secure reduction of weak $\binom{N}{1}$-OT^L to $\binom{n}{1}$-OT^ℓ such that*

- *it uses $\frac{L}{\ell} \cdot \frac{N-1}{n-1}$ invocations of $\binom{n}{1}$-OT^ℓ.*
- *the sender uses $\frac{L(N-n)}{n-1}$ random bits.*

*Moreover, for $L = \ell$, the reduction actually reduces (*strong*) $\binom{N}{1}$-OT^ℓ to $\binom{n}{1}$-OT^ℓ.*

Proof: We start with $L = \ell$, i.e. a reduction of (strong) $\binom{N}{1}$-OT$^\ell$ to $\binom{n}{1}$-OT$^\ell$, making $\alpha = \frac{N-1}{n-1}$ invocations and using $\frac{\ell(N-n)}{n-1}$ random bits for Alice. Let $w = w_1, \ldots, w_N$ be Alice's N strings of length ℓ each, and let i be Bob's index.

Protocol $P(w, i)$:

1. Alice chooses $(\alpha - 1)$ random ℓ-bit strings $x_1, \ldots, x_{\alpha-1}$ using $\ell(\alpha - 1) = \frac{\ell(N-n)}{n-1}$ random bits. Set $x_0 = 0^\ell$, $x_\alpha = w_N$.
2. Perform α invocations of $\binom{n}{1}$-OT$^\ell$, where transfer $j = 0 \ldots (\alpha - 1)$ is:

$$\binom{n}{1}\text{-OT}^\ell \left[w_{j(n-1)+1} \oplus x_j, \ldots, w_{(j+1)(n-1)} \oplus x_j,\ x_{j+1} \oplus x_j \right]$$

   Let z_j be the value Bob reads from the j-th invocation, described next.
3. Let $j_0 \in \{0 \ldots (\alpha - 1)\}$ be the index of the OT box which has the XOR-ed value of w_i ($\lfloor \frac{i-1}{n-1} \rfloor$, if $i \neq N$, and $(\alpha - 1)$, otherwise). Bob reads the value $z_{j_0} = w_i \oplus x_{j_0}$ from transfer j_0 and values $z_j = x_{j+1} \oplus x_j$ for all $j \neq j_0$.
4. Bob outputs $\bigoplus_{j=0}^{j_0} z_j$.

The special case of $n = 2$ (originally considered in [5, 4] and yielding $(N-1)$ invocations and $(N-2)$ ℓ-bit random strings) is demonstrated in Figure 1. The intuition behind this protocol (for any n) is the following. As long as Bob reads the "right-most" value $x_{j+1} \oplus x_j$, he does not learn anything about all the strings w_i used inside the first $(j+1)$ transfers. As soon as he learns some $w_i \oplus x_j$ instead of $x_{j+1} \oplus x_j$, he learns w_i, but "misses" all the future w_k for $k > i$ as he "missed" x_{j+1}. We now formally prove that the above protocol indeed implements (strong) $\binom{N}{1}$-OT$^\ell$.

The Correctness Property (P1) is clear since $(w_i \oplus x_{j_0}) \oplus (x_{j_0} \oplus x_{j_0-1}) \oplus \ldots (x_2 \oplus x_1) \oplus x_1 = w_i$. The Receiver Privacy (P2) is clear as well since the scheme is one-way and, as we just saw, Bob can recover any w_i. We now show the main condition (P3).

Let $W = W_1, \ldots, W_N$ be chosen at random as well as Alice's random string $R = X_1, \ldots, X_{\alpha-1}$. Let V be the random variable containing all the (αn) values of the $\binom{n}{1}$-OT$^\ell$ boxes. We can assume w.l.o.g. that in

each of the α OT boxes, Bob indeed read one entire ℓ-bit string that he chose (he can not learn more and it "does not hurt" to learn as much as possible). Thus, define V_r to be the α-tuple of ℓ-bit strings that Bob read, i.e. everything that Bob learned from the protocol. Let $t_0, \ldots, t_{\alpha-1}$, where $t_j \in [n]$, be the (random variables denoting the) indices of the α strings that Bob read.

Let j_0 be the smallest number such that $t_{j_0} \neq n$, if it exists. Otherwise, $j_0 = \alpha - 1$. Thus, Bob learned $X_1, X_1 \oplus X_2, \ldots, X_{j_0-2} \oplus X_{j_0-1}$ and some $W_i \oplus X_{j_0-1}$. Clearly, this enables him to reconstruct W_i (the exceptional case of all $t_j = n$ falls here as well giving Bob W_N). We let $\tilde{I} = i$. First of all, $\tilde{I}$ is *independent* from W. Indeed, Bob choose to read index t_{j_0} in the j_0-th invocation of $\binom{n}{1}$-OT$^\ell$ only based on his random coins and $X_1, X_1 \oplus X_2, \ldots, X_{j_0-2} \oplus X_{j_0-1}$, which does not depend on W. Thus, it suffices to show that $\mathbf{I}(V_r; W \mid W_{\bar{I}}) = 0$. But we already observed that $W_{\bar{I}}$ is determined from V_r. Hence, using Lemma 1 (equations 4 and 3),

$$\begin{aligned} \mathbf{I}(V_r \ ; \ W) &= \mathbf{I}((V_r, W_{\bar{I}}) \ ; \ W) = \mathbf{I}(W_{\bar{I}} \ ; \ W) + \mathbf{I}(V_r \ ; \ W \mid W_{\bar{I}}) \\ &= \ell + \mathbf{I}(V_r \ ; \ W \mid W_{\bar{I}}) \end{aligned}$$

Thus, we only need to show that $\mathbf{I}(V_r; W) = \ell$, i.e. to establish the weak property (P3′). Intuitively, Bob always learns some $W_{\bar{I}}$, i.e. ℓ bits of information. So if we show that he does not learn more than ℓ bits of information, we know that the only thing he learned was that *one* string $W_{\bar{I}}$. We proceed by showing a sequence of easy claims.

Local Claim 1: W is a function of V, i.e.

$$\mathbf{H}(W \mid V) = 0 \tag{7}$$

Proof: We already saw from correctness that V determines each string W_i. □

Local Claim 2:

$$\mathbf{H}(V \backslash V_r \mid V_r) = \ell(N-1) \tag{8}$$

Proof: We show that all (αn) ℓ-bit strings of V are totally independent when W and R are randomly chosen. Let us view each such string in V as an $(N + \alpha - 1)$-dimensional vector over $\mathbb{Z}_2$ by taking the characteristic vector of the equation defining this string. Since all W_i and X_j are chosen randomly, our strings are independent if and only if the corresponding vectors are *linearly independent*. Assume that some linear combination of vectors in V is zero. This combination cannot include a vector depending on some W_i as there is only one such vector in V. And the remaining vectors $X_1, X_1 \oplus X_2, \ldots, X_{\alpha-2} \oplus X_{\alpha-1}$ are clearly linearly independent. And since our disjoint split of V into V_r and $V \backslash V_r$ does not depend on $V \backslash V_r$, we get that $V \backslash V_r$ is independent of V_r, so by Lemma 1 (equation 5 and 8),

$$\mathbf{H}(V \backslash V_r \mid V_r) = \mathbf{H}(V \backslash V_r) = |V \backslash V_r| = \ell(n-1)\alpha = \ell(N-1)$$

□

Local Claim 3: $V \backslash V_r$ is determined from W and V_r, i.e.

$$\mathbf{H}(V \backslash V_r \mid (V_r, W)) = 0 \tag{9}$$

Proof: The knowledge of W and any string $W_i \oplus X_{\alpha-1}$ in the last $\binom{n}{1}$-OT$^\ell$ box (which we have from V_r) determines $X_{\alpha-1}$. Knowing $X_{\alpha-1}$, W and any string of the form $z \oplus X_{\alpha-2}$ from the next to last $\binom{n}{1}$-OT$^\ell$ box (which we have from V_r where z is either some W_i or $X_{\alpha-1}$) enables one to deduce $X_{\alpha-2}$. Continuing this way, we determine X_1 from the first $\binom{n}{1}$-OT$^\ell$ box which allows us to reconstruct the whole $V \backslash V_r$. □

Combining Local Claims 1,2,3 and using Lemma 1 (equations 8, 1, 2 and 3),

$$\begin{aligned} \ell N &= \mathbf{H}(W) = \mathbf{H}(W) - \mathbf{H}(W \mid V) = \mathbf{I}(V; W) = \mathbf{I}(V_r; W) + \mathbf{I}(V \backslash V_r; W \mid V_r) \\ &= \mathbf{I}(V_r; W) + \mathbf{H}(V \backslash V_r \mid V_r) - \mathbf{H}(V \backslash V_r \mid (V_r, W)) = \mathbf{I}(V_r; W) + \ell(N-1) \end{aligned}$$

Hence, $\mathbf{I}(V_r; W) = \ell$ indeed. This completes the proof of correctness when $L = \ell$.

For $\ell < L$ we give a trivial protocol that sacrifices the strong property (P3) leaving only (P3′). The protocol simply splits each of the strings of the database into L/ℓ disjoint parts of length ℓ each, and performs the previous protocol implementing $\binom{N}{1}$-OT$^\ell$ using $\binom{n}{1}$-OT$^\ell$. It uses $\frac{L}{\ell} \cdot \frac{N-1}{n-1}$ invocations of $\binom{n}{1}$-OT$^\ell$ and $\frac{L}{\ell} \cdot \frac{\ell(N-n)}{n-1} = \frac{L(N-n)}{n-1}$ random bits as claimed. The correctness is clear except Alice's privacy. We clearly loose the strong property (P3) as Bob can learn up to L/ℓ different blocks of length ℓ from different strings. However, weak property (P3′) still holds as the L/ℓ groups of boxes are totally independent, and from each of them Bob can learn at most ℓ bits about W, i.e. a total of at most $\ell \cdot \frac{L}{\ell} = L$ bits. ■

4.2 Reducing $\binom{N}{1}$-OT^L to $\binom{n}{1}$-OT$^\ell$ for $L > \ell$

We just saw that the bound of Theorem 1 is tight for reducing (strong) $\binom{N}{1}$-OT^L to $\binom{n}{1}$-OT$^\ell$ when $L = \ell$. We now generalize another reduction of [5] and [4] to show that the bound is always tight up to a constant factor. For this we need to define the notion of a *zigzag function*.

4.2.1 Zigzag Functions

Given $z = z_1 \dots z_S \in \{0,1\}^S$ and $J = \{i_1, \dots, i_j \mid i_1 < \dots < i_j\} \subseteq [S]$, we let $[z]_J = z_{i_1} \dots z_{i_j}$ be the bits of z in J. Let $f : \{0,1\}^S \to \{0,1\}^L$ be a surjective function, W be chosen uniformly at random from $\{0,1\}^L$, and Z be a random pre-image of W (which exists due to surjectivity of f).

Definition 2 *A set $J \subseteq [S]$ is said to* bias *f if $[Z]_J$ reveals some information about $W = f(Z)$:*

$$\mathbf{I}(W; [Z]_J) > 0$$

In other words, if J does *not* bias f, observing $[Z]_J$ gives no information about W.

Definition 3 *A surjective function $f : \{0,1\}^S \to \{0,1\}^L$ is called an* (S, L)-zigzag *function if for any partition of $[S]$ into disjoint subsets $J_1, \dots, J_N$,* at most one *of $J_1, \dots, J_N$ biases f.*

Notice that it suffices to check the definition of a zigzag function only for $N = 2$, i.e. partitions of $[S]$ into two disjoint subsets (since if J_i and J_k bias f, then so do J_i and $[S] \backslash J_i$). Aside from verifying the existence of zigzag functions, the objective is to make S as small as possible, and we will soon see the reason why.

A particular nice class of zigzag functions are *linear* zigzag functions, which are given by an $L \times S$ binary matrix M which defines $f(z) = M \cdot z$ (here the operations are in $GF(2)$). Notice that the matrix M also defines an *error-correcting code* C in $\{0,1\}^S$, where the codewords are all the elements of the form $u \cdot M$, where $u \in \{0,1\}^L$. Brassard, Crépeau and Sántha [5] showed an easily verified but surprising connection between f being a zigzag function and the properties of C.

Lemma 3 ([5]) *$f(z) = M \cdot z$ is an (S, L)-zigzag function if and only if and only if $C = \{u \cdot M \mid u \in \{0,1\}^L\}$ is a* self-intersecting code*, that is every non-zero $c_1, c_2 \in C$ have at least one common non-zero coordinate.*[5]

Self-intersecting codes have been studied earlier (for instance, by [7]). In particular, it is known that for any $\gamma > \log_{4/3} 4 \approx 4.8188$, a *random* $\gamma L \times L$ binary matrix M defines a self-intersecting code (or a zigzag function) with probability exponentially close to 1.[6] In particular,

Theorem 4 ([7, 5]) *For any L there exist $(\gamma L, L)$-zigzag functions, where $\gamma < 5$.*

[5] The reason such code is called self-intersecting is that if we view each non-zero codeword as a subset of $\{0,1\}^S$ (by looking at its characteristic vector), the condition above says that any two non-empty codewords intersect.

[6] Brassard et al [5] give efficient deterministic algorithms to construct zigzag functions with much larger constants γ, but we are not concerned with efficiency or constuctiveness in order to match our lower bound.

4.2.2 A Simple Protocol using Zigzag Functions

We can now give a simple one-way reduction from $\binom{N}{1}$-OT^L to $\binom{N}{1}$-OT$^\ell$ slightly generalizing the reductions of [4, 5]. We let $f : \{0,1\}^S \to \{0,1\}^L$ be an (S, L)-zigzag function with $S = O(L)$. Let $B_j = \{j\ell+1, \ldots, (j+1)\ell\}$, $j = 0, \ldots, L/\ell - 1$. In other words, we split $[S] = \{1, \ldots, S\}$ into $\alpha = S/\ell$ consecutive blocks of size ℓ each. Given $z \in \{0,1\}^S$ we let $[z]_j = [z]_{B_j}$ be the restriction of z to its ℓ bits in B_j.

Protocol $Q(w, i)$:

1. Alice chooses a random z_i such that $f(z_i) = w_i$, $\forall i \in [N]$.
2. Perform α invocations of $\binom{N}{1}$-OT$^\ell$ where transfer $j = 0 \ldots (\alpha - 1)$ is:

$$\binom{N}{1}\text{-OT}^\ell \; [\; [z_1]_j, \ldots, \; [z_N]_j \;]$$

3. Bob reads i-th value $[z_i]_j$ in each OT, reconstructs z_i and outputs $f(z_i)$.

Let J_k be the union of all B_j such that Bob read $[z_k]_j$ in the j-th OT. Then Bob learned $[z_k]_{J_k}$ for all k. Notice that $J_1, \ldots, J_N$ form a disjoint partition of $[S]$. Since f is a zigzag function, at most one of J_k biases f, say J_t. Then Bob does not learn any information about w_k for any $k \neq t$, since the distribution of $[z_k]_{J_k}$ is independent of w_k. It is a trivial routine matter (much simpler than for the protocol from the previous section) to transform this intuition into a formal proof, and this was indeed done in [5].

We notice that the number of $\binom{N}{1}$-OT$^\ell$ invocations is S/ℓ, and that is why we need S to be as small as possible. Since $S = O(L)$ by Theorem 4, we get:

Theorem 5 *There exists a one-way reduction of $\binom{N}{1}$-OT^L to $\binom{N}{1}$-OT$^\ell$ using $O(L/\ell)$ invocations of the latter.*

By finally combining the combining the above reduction with the reduction from Theorems 3 (from $\binom{N}{1}$-OT$^\ell$ to $\binom{n}{1}$-OT$^\ell$), we get

Corollary 1 *There exists a one-way reduction of $\binom{N}{1}$-OT^L to $\binom{n}{1}$-OT$^\ell$ using $O(\frac{L}{\ell} \cdot \frac{N-1}{n-1})$ invocations of the latter.*

To summarize, the bound of Theorem 1 is always tight up to a constant factor and is exactly tight for $L = \ell$ and for the case of weak $\binom{N}{1}$-OT^L.

5 Concluding Thoughts

Typically, 1-out-of-2 OT is considered as a basic primitive, and efficient cryptographic protocols have been designed for this case based on various cryptographic assumptions (for example, those of [1] and [15]). Thus, in order to implement general 1-out-of-N OT, the following methodology is suggested: use information-theoretic reduction to 1-out-of-2 OT, and then use a cryptographic protocol for every invocation of the latter. While this methodology works and is often used, there are alternative (and often more efficient) ways to build 1-out-of-N OT. In particular, there are very efficient "direct" cryptographic protocols for $\binom{N}{1}$-OT^L based on various assumptions. For example, Dodis, Halevi and Rabin [13] give a simple $\binom{N}{1}$-OT^L protocol based on any "blindable" encryption scheme (e.g., El-Gamal [14] or Goldwasser-Micali [19]), while Naor [24] recently gave a very efficient $\binom{N}{1}$-OT^L protocol based on the Diffie-Helman assumption. Alternatively, Naor and Pinkas [25] gave a very efficient "cryptographic reduction" from $\binom{N}{1}$-OT^L to $\binom{2}{1}$-OT^L which uses only $\log N$ invocations of $\binom{2}{1}$-OT^L (compare with the lower bound of $(N-1)$ given by Theorem 1) in addition to $O(N)$ invocations of a pseudorandom function (which are considered to be more efficient than $\binom{2}{1}$-OT^L). Of course, this "gap" from $\log N$ to N is very artifical and not well defined once we use computational assumptions (in particular, we can build the complex OT directly), and makes sense only

in terms minimizing the amount of work outside of performing simpler OTs (e.g., using relatively inexpensive evaluations of a pseudorandom function).

While these cryptographic results surpass the lower bounds we established in Section 3 (in fact, the lower bounds do not make sense if we use cryptographic assumptions), the lower bounds are still quite meaningful. For one thing, they show that simple but seemingly inefficient reductions of complex to simpler OT's are actually the best we can hope to achieve. On the other side, they show that there are some non-trivial information-theoretic limitations of expressing a complex OT in terms of a simpler one, forcing one to either build complex OT's directly, or to use "cryptographic reductions", or to settle for somewhat inefficient performance when building complex OT's. In particular, the attractive methodology of building only $\binom{2}{1}$-OT might not be the best one in practice.

References

[1] M. Bellare and S. Micali. Non-interactive Oblivious Transfer and Applications. In *Advances in Cryptology: Proceedings of Crypto '90*, pp. 547–559, Springer-Verlag, 1990.

[2] M. Blum. How to Exchange (Secret) Keys. In *ACM Transactions of Computer Systems*, vol. 1, No. 2, pp. 175–193, May 1983.

[3] G. Brassard and C. Crépeau. Oblivious Transfers and Privacy Amplification. In *Advances in Cryptology: Proceedings of Eurocrypt '97*, Springer-Verlag, pp. 334–347, 1997.

[4] G. Brassard, C. Crépeau and J. Robert. Information theoretic reductions among disclosure problems. In *27th Symp. of Found. of Computer Sci.*, pp. 168–173, IEEE, 1986.

[5] G. Brassard, C. Crépeau and M. Sántha. Oblivious Transfers and Intersecting Codes. In *IEEE Transaction on Information Theory, special issue in coding and complexity*, Volume 42, Number 6, pp. 1769–1780, 1996.

[6] C. Cachin. On the foundation of Oblivious Transfer. In *Advances in Cryptology: Proceedings of Eurocrypt '98*, Springer-Verlag, pp. 361–374, 1998.

[7] G. Cohen and A. Lempel. Linear Intersecting Codes. In *Discrete Mathematics*, 56:35–43, 1985.

[8] T. Cover and J. Thomas. Elements of Information Theory. Wiley & Sons, New York, 1991.

[9] C. Crépeau. Equivalence between two flavors of oblivious transfers. In *Advances in Cryptology: Proceedings of Crypto '87*, volume 293 of Lecture Notes in Computer Science, pp. 350-354, Springer-Verlag, 1988.

[10] C. Crépeau. A zero-knowledge poker protocol that achieves confidentiality of the players' strategy or how to achieve an electronic poker face. In *Advances in Cryptology: Proceedings of Crypto '86*, pp. 239–247. Springer-Verlag, 1987.

[11] C. Crépeau and J. Kilian. Weakening security assumptions and oblivious transfer. In *Advances in Cryptology: Proceedings of Crypto '88*, volume 403 of Lecture Notes in Computer Science, pp. 2-7, Springer-Verlag, 1990.

[12] I. Damgård, J. Kilian and L. Salvail. On the (im)possibility of basing oblivious transfer and bit commitment on weakened security assumptions. In *Advances in Cryptology: Proceedings of Eurocrypt '99*, Springer-Verlag, pp. 56–73, 1999.

[13] Y. Dodis, S. Halevi and T. Rabin. A Cryptographic Solution to a Game Theoretic Problem, In *Advances in Cryptology: Proceedings of Crypto '00*, volume 1880 of Lecture Notes in Computer Science, pp. 112-130, Springer-Verlag, 2000.

[14] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In *Advances in Cryptology – CRYPTO '84*, volume 196 of *Lecture Notes in Computer Science*, pages 10–18. Springer-Verlag, 1985.

[15] S. Even, O. Goldreich and A. Lempel. A Randomized Protocol for Signing Contracts. In *Advances of Cryptology: Proceedings of Crypto '83*, Plenum Press, New York, pp. 205-210, 1983.

[16] M. Fisher, S. Micali and C. Rackoff. A Secure Protocol for the Oblivious Transfer. In *Journal of Cryptology*, vol. 9, No. 3 pp. 191–195, 1996.

[17] O. Goldreich, S. Micali and A. Wigderson. How to play any mental game, or: A completeness theorem for protocols with honest majority. In *Proceedings of 19th Annual Symp. on Theory of Computing*, 218-229, 1987.

[18] O. Goldreich, R. Vainish. How to Solve any Protocol Problem - An Efficiency Improvement. In *Advances of Cryptology: Proceedings of Crypto'87*, pp 73–86.

[19] S. Goldwasser and S. Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28(2):270–299, April 1984.

[20] S. Goldwasser, S. Micali and C. Rackoff. The knowledge complexity of interactive proof-systems. In *SIAM Journal on Computing*, 18:186-208, 1989.

[21] J. Kilian. Founding Cryptography on Oblivious Transfer. In *Proceedings of 20th Annual Symp. on Theory of Computing*, pp. 20–31, 1988.

[22] J. Kilian, S. Micali and R. Ostrovsky. Minimum Resource Zero-Knowledge Proofs. In *Proceedings of 30th Annual Symp. on Foundations of Computer Science*, pp. 474–479, 1989.

[23] U. Maurer. Information-Theoretic Cryptography. In *Advances in Cryptology: Crypto' 99 Proceedings*, pp. 47–64, Springer-Verlag, 1999.

[24] M. Naor. Personal Communication.

[25] M. Naor, and B. Pinkas. Oblivious Transfer and Polynomial Evaluation. In *Proceedings of 31th Annual Symp. on Theory of Computing*, pp. 245–254, 1999.

[26] H. Nurmi, A. Salomaa and L. Santean. Secret ballot elections in computer networks. In *Computer and Security*, volume 10, No. 6, pp. 553-560, 1991.

[27] M. Rabin. How to Exchange Secrets by Oblivious Transfer. In *Technical Memo TR-81*, Aiken Computation Laboratory, Harvard University, 1981.