New Monotones and Lower Bounds in Unconditional Two-Party Computation

Stefan Wolf Jürg Wullschleger

Département d'Informatique et R.O.
Université de Montréal, Québec, Canada.
{wolf,wullschj}@iro.umontreal.ca

Abstract. Since bit and string *oblivious transfer* and *commitment*, two primitives of paramount importance in secure two- and multi-party computation, cannot be realized in an unconditionally secure way for both parties from scratch, *reductions* to weak information-theoretic primitives as well as between different variants of the functionalities are of great interest. In this context, we introduce three independent *monotones*—quantities that cannot be increased by any protocol—and use them to derive lower bounds on the *possibility* and *efficiency* of such reductions. An example is the transition between different versions of oblivious transfer, for which we also propose a new protocol allowing to increase the number of messages the receiver can choose from at the price of a reduction of their length. Our scheme matches the new lower bound and is, therefore, optimal.

1 Introduction, Motivation, and Main Results

The advantage of *unconditional* or *information-theoretic* security—as compared to computational security—is that it does not depend on any assumption on an adversary's computing power or memory space, nor on the hardness of any computational problem. Its disadvantage, on the other hand, is that it cannot be realized simply from scratch. This is why *reductions* are of great interest and importance in this context: Which functionality can be realized from which other? If a reduction is possible in principle, what is the best efficiency, i.e., the minimum number of instances of the initial primitive required per realization of the target functionality?

Two tasks of particular importance in secure two-party computation are *oblivious transfer* and *bit commitment*. Both primitives are known to be impossible to realize from scratch in an unconditionally secure way for both parties by any (classical or even quantum) protocol. On the other hand, they *can* be realized from noisy channels [6], [7], weak versions of oblivious transfer [3], correlated pieces of information [18], or the assumption that one of the parties' memory space is limited.

For the same reason, reductions between different variants of oblivious transfer are of interest as well: chosen 1-out-of-2 oblivious transfer from Rabin oblivious transfer [5], string oblivious transfer from bit oblivious transfer [3], 1-out-of-n

oblivious transfer from 1-out-of-2 oblivious transfer, oblivious transfer from A to B from oblivious transfer from B to A [8], [19], and so forth. A number of lower bounds in the context of such reductions have been given, based on information-theoretic arguments [9], [13].

With respect to information-theoretic reductions between cryptographic and information-theoretic functionalities, quantities which never increase during the execution of a protocol—so-called *monotones* [4]—are of great importance. In *key agreement*, for instance, two parties A and B can start with correlated pieces of information X and Y, respectively, and try to generate a secret key S by public communication such that an adversary E, who initially knows a third random variable Z, is virtually ignorant about S. It has been shown in [16] that the *intrinsic information* [14] of A's and B's entire knowledge, given E's, is a monotone, i.e., cannot increase. This immediately leads to the following bound on the size of the generated key: $H(S) \leq I(X;Y{\downarrow}Z)$.

The main results of our paper are the following.

Three monotones of unconditional two-party computation.
In Section 3, we define three information-theoretic quantities (the underlying notions are introduced in Section 2) and prove them to be monotones: No protocol allows for increasing them.

Lower bounds for oblivious-transfer reductions.
In Section 4.1, we derive a new lower bound on the efficiency of reductions from one variant of oblivious transfer to another, and of realizing oblivious transfer from shared correlated pieces of information.

Optimally trading message length for choice in oblivious transfer.
In Section 4.2, we present a new protocol allowing for increasing the number of messages from which the receiver can choose at the price of a reduction of their length. Our lower bound shows that the protocol is optimal.

New error bounds for bit commitment.
In Section 5, we show new lower bounds on the probability of failure of any protocol for bit commitment based on correlated pieces of information.

2 Preliminaries: Common and Dependent Parts

As a preparation, we introduce two notions, namely the *common part* $X \wedge Y$ and the *dependent parts* $X \searrow Y$ and $Y \searrow X$ of two random variables X and Y. In the context of cryptography, the notions have first been used in [10], [12], [18]. Both notions have appeared previously in other information-theoretic contexts [11], the latter under the name of *sufficient statistics*.

2.1 Common Part

Let X and Y be two random variables with joint distribution P_{XY}. Intuitively, the common part $X \wedge Y$ is the maximal element of the set of all random variables that can be generated both from X and from Y.

Definition 1. [18] *Let X and Y be random variables with (disjoint) ranges $\mathcal{X}$ and $\mathcal{Y}$ and distributed according to P_{XY}. Then $X \wedge Y$, the* common part *of X and Y, is constructed in the following way:*

- *Consider the bipartite graph G with vertex set $\mathcal{X} \cup \mathcal{Y}$, and where two vertices $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ are connected by an edge if $P_{XY}(x, y) > 0$ holds.*
- *Let $f_X : \mathcal{X} \to 2^{\mathcal{X} \cup \mathcal{Y}}$ be the function that maps a vertex $v \in \mathcal{X}$ of G to the set of vertices in the connected component of G containing v. Let $f_Y : \mathcal{Y} \to 2^{\mathcal{X} \cup \mathcal{Y}}$ be the function that does the same for a vertex $w \in \mathcal{Y}$ of G.*
- *$X \wedge Y := f_X(X) = f_Y(Y)$.*

Note that $X \wedge Y$ is symmetric—i.e., $X \wedge Y \equiv Y \wedge X$ [1]. There exist functions f_X and f_Y with $X \wedge Y = f_X(X) = f_Y(Y)$. Hence, $X \wedge Y$ can be calculated both from X and from Y.

Lemma 1. [18] *For all X, Y, and $\overline{C}$ for which there exist functions $\overline{f}_X$ and $\overline{f}_Y$ such that $\overline{C} = \overline{f}_X(X) = \overline{f}_Y(Y)$ holds, there exists a function g with $\overline{C} = g(X \wedge Y)$.*

2.2 Dependent Part

Intuitively, the *dependent part* of X from Y, denoted $X \searrow Y$, is the minimal element of the set of all random variables K that can be generated from X and are such that $X \longleftrightarrow K \longleftrightarrow Y$ is a Markov chain.

Definition 2. [10] *Let X and Y be two random variables, and let $f(x) = P_{Y|X=x}$. The* dependent part of X from Y *is defined as $X \searrow Y := f(X)$.*

Lemma 2 shows that all of X that is dependent on Y is included in $X \searrow Y$, i.e., more formally, $I(X; Y | X \searrow Y) = 0$ holds or, equivalently, X, $X \searrow Y$, and Y form a Markov chain.

Lemma 2. [10] *For all X and Y, $X \longleftrightarrow (X \searrow Y) \longleftrightarrow Y$ is a Markov chain.*

On the other hand, there does not exist a random variable with the same properties that is "smaller" than $X \searrow Y$.

Lemma 3. [18] *Let X, Y, and $\overline{K}$ be random variables such that there exists a function $\overline{f}$ such that $\overline{K} = \overline{f}(X)$ and $X \longleftrightarrow \overline{K} \longleftrightarrow Y$ hold. Then there exists a function g with $X \searrow Y = g(\overline{K})$.*

[1] We say that two random variables A and B are equivalent, denoted by $A \equiv B$, if there exists a bijective function $g : \mathcal{A} \to \mathcal{B}$ such that $B = g(A)$ holds with probability 1.

3 Three Two-Party-Protocol Monotones

In this section we show that the following three quantities are monotones, i.e., cannot increase during the execution of any protocol based on (noiseless) communication and (lossless) processing (where X' and Y' are the random variables summarizing the entire information accessible to A and B, respectively):

$$H(Y' \searrow X'|X') \ ,$$
$$H(X' \searrow Y'|Y') \ ,$$
$$I(X'; Y'|X' \wedge Y') \ .$$

We first show that local randomness generation and data processing, and second, that noiseless bi-directional communication do not allow for increasing any of these quantities.

3.1 Invariance Under Randomness Generation and Data Processing

Lemma 4. *Let X, Y, and Z be random variables such that $X \longleftrightarrow Y \longleftrightarrow Z$ is a Markov chain. Then we have*

$$X \searrow [Y, Z] \equiv X \searrow Y \ .$$

Proof. We have $P_{YZ|X=x} = P_{Y|X=x}P_{Z|Y}$. Therefore, for all $x, x' \in \mathcal{X}$, the function $P_{YZ|X=x}$ is different from $P_{YZ|X=x'}$ if and only if $P_{Y|X=x}$ is different from $P_{Y|X=x'}$. □

Lemma 5. *Let W, X, and Y be random variables such that $W \longleftrightarrow X \longleftrightarrow Y$ is a Markov chain. Then we have*

$$[W, X] \searrow Y \equiv X \searrow Y \ .$$

Proof. We have $P_{Y|W=w,X=x} = P_{Y|X=x}$. Therefore, for all $w, w' \in \mathcal{W}$ and $x, x' \in \mathcal{X}$, the function $P_{Y|W=w,X=x}$ is different from $P_{Y|W=w',X=x'}$ if and only if $P_{Y|X=x}$ is different from $P_{Y|X=x'}$. □

Lemma 6. *Let X, Y, and Z be random variables such that $X \longleftrightarrow Y \longleftrightarrow Z$ is a Markov chain. Then we have*

$$X \wedge [Y, Z] \equiv X \wedge Y \ .$$

Proof. We have $P_{XYZ} = P_{XY}P_{Z|Y}$. Let us look at the connection graph between all the values x and (y, z) for which $P_X(x) > 0$ and $P_{YZ}(y, z) > 0$ hold. Then x and (y, z) are connected if and only if $P_{XYZ}(x, y, z) > 0$ holds. Since $P_{Z|Y}(z, y) > 0$, this holds if and only if $P_{XY}(x, y) > 0$ holds. Hence, $X \wedge [Y, Z] \equiv X \wedge Y$. □

Theorem 1 shows that local data processing does not increase any of the quantities in question. It is a direct consequence of Lemmas 4, 5, and 6.

Theorem 1. *Let X, Y, and Z be random variables with $X \longleftrightarrow Y \longleftrightarrow Z$. Then we have*

$$H([Y,Z] \searrow X|X) = H(Y \searrow X|X) \ ,$$
$$H(X \searrow [Y,Z]|[Y,Z]) = H(X \searrow Y|Y) \ ,$$
$$I(X;[Y,Z]|X \wedge [Y,Z]) = I(X;Y|X \wedge Y) \ .$$

3.2 No Increase by Communication

We now show that the same holds with respect to noise-free communication between A and B. We first prove three lemmas.

Lemma 7. *Let X and Y be random variables and f a function. Then*

$$X \searrow [Y, f(X)] \equiv [X \searrow Y, f(X)] \ .$$

Proof. Let $h_1(X) := X \searrow [Y, f(X)]$ and $h_2(X) := [X \searrow Y, f(X)]$, and let $F = f(X)$. We have $P_{YF|X} = P_{Y|X}P_{F|X}$. For all x, x' with $h_1(x) = h_1(x')$, we have $P_{YF|X=x} = P_{YF|X=x'}$, which holds exactly if $P_{Y|X=x} = P_{Y|X=x'}$ and $f(x) = f(x')$ hold, which is equivalent to $h_2(x) = h_2(x')$. Hence, $X \searrow [Y, f(X)] \equiv [X \searrow Y, f(X)]$. □

Lemma 8. *Let X and Y be random variables and f a function. Then there exists a function g such that*

$$[Y, f(X)] \searrow X = g([Y \searrow X, f(X)]) \ .$$

Proof. Let $h_1(X,Y) := [Y, f(X)] \searrow X$ and $h_2(X,Y) := [Y \searrow X, f(X)]$. For all x, x', y, and y' with $h_2(x,y) = h_2(x',y')$, we have $P_{X|Y=y} = P_{X|Y=y'}$ and $f(x) = f(x')$. It follows $P_{X|Y=y,f(X)=f(x)} = P_{X|Y=y',f(X)=f(x)}$, and, hence, $h_1(x,y) = h_1(x',y')$. Therefore, there must exist a function g with $h_1 = g \circ h_2$. □

Lemma 9. *Let X, Y, and Z be random variables. There exists a function f such that*

$$X \wedge Y = f([X,Z] \wedge Y) \ .$$

Proof. $X \wedge Y$ can be calculated from X, and, hence, also from $[X,Z]$. The statement now follows from Lemma 1. □

Theorem 2 states that noiseless communication between the two parties cannot increase any of the quantities in question.

Theorem 2. *Let X and Y be two random variables and f a function. Then we have*

$$H([Y, f(X)] \searrow X|X) \leq H(Y \searrow X|X) \ ,$$
$$H(X \searrow [Y, f(X)]|Y, f(X)) \leq H(X \searrow Y|Y) \ ,$$
$$I(X;[Y, f(X)|X \wedge [Y, f(X)]) \leq I(X;Y|X \wedge Y) \ .$$

Proof. Using Lemmas 7, 8, and 9, we obtain

$$\begin{aligned}
H([Y, f(X)] \searrow X|X) &\leq H([Y \searrow X, f(X)]|X) \\
&= H(Y \searrow X|X)
\end{aligned}$$

$$\begin{aligned}
H(X \searrow [f(X), Y]|f(X), Y) &= H([X \searrow Y, f(X)]|f(X), Y) \\
&= H(X \searrow Y|f(X), Y) \\
&\leq H(X \searrow Y|Y)
\end{aligned}$$

$$\begin{aligned}
I(X; [f(X), Y]|X \wedge [f(X), Y]) &\leq I(X; [f(X), Y]|f(X), X \wedge Y) \\
&= I(X; Y|f(X), X \wedge Y) \\
&\leq I(X; Y|X \wedge Y)
\end{aligned}$$

□

Corollary 1 is a direct consequence of Theorems 1 and 2.

Corollary 1. *Let X and Y be two parties' entire knowledge* before*, and X' and Y'* after *the execution of a protocol including local data processing and noiseless communication. Then we have*

$$\begin{aligned}
H(X' \searrow Y'|Y') &\leq H(X \searrow Y|Y) \ , \\
H(Y' \searrow X'|X') &\leq H(Y \searrow X|X) \ , \\
I(X'; Y'|X' \wedge Y') &\leq I(X; Y|X \wedge Y) \ .
\end{aligned}$$

4 Oblivious Transfer: Lower Bounds and an Optimal Reduction

4.1 New Bounds on Oblivious-Transfer Reductions

In m-out-of-n k-string oblivious transfer, denoted $\binom{n}{m}$-OT^k, the sender inputs n k-bit messages out of which the receiver can choose to read m, but does not obtain any further information about the messages; the sender, on the other hand, does not obtain any information on the receiver's choice.

In [1], it has been shown that $\binom{2}{1}$-OT^1 is *equivalent* to pieces of information with a certain distribution (in other words, oblivious transfer can be precomputed and stored). This result generalizes to $\binom{n}{m}$-OT^k in a straight-forward way. By determining the corresponding values of the three monotones derived in Section 3 we can, thus, obtain lower bounds on the reducibility between different variants of oblivious transfer. The bound of Theorem 4 is an improvement on an earlier bound by Dodis and Micali [9].

Theorem 3. *Assume that there exists a protocol for realizing unconditionally secure* $\binom{N}{M}$-OT^K *from distributed random variables* X *and* Y*. Then we have*

$$\begin{aligned}(N-M)K &\leq H(X \searrow Y|Y) \ , \\ \log \binom{N}{M} &\leq H(Y \searrow X|X) \ , \\ MK &\leq I(X;Y|X \wedge Y) \ .\end{aligned}$$

Proof. As mentioned, $\binom{N}{M}$-OT^K can be stored. More specifically, the corresponding random variables X' and Y' arise when $\binom{N}{M}$-OT^K is executed with random and independent inputs. We have $H(X' \searrow Y'|Y') = (N-M)K$, $I(X';Y'|X' \wedge Y') = MK$, and $H(Y' \searrow X'|X') = \log \binom{N}{M}$. The assertion now follows from Corollary 1. □

Theorem 4. *Assume that there exists a protocol for realizing unconditionally secure* $\binom{N}{M}$-OT^K *from* t *instances of* $\binom{n}{m}$-OT^k*. Then we have*

$$t \ \geq \ \max\left(\frac{(N-M)K}{(n-m)k}, \frac{\log \binom{N}{M}}{\log \binom{n}{m}}, \frac{MK}{mk}\right) \ .$$

Proof. Since $\binom{n}{m}$-OT^k is *equivalent* to the pieces of information obtained when the primitive is used with random inputs, we can assume that A and B start the protocol with such random variables X_i and Y_i, respectively, for $i = 1, \ldots, t$. (The first step in this protocol can be to restore $\binom{n}{m}$-OT^k from the shared information.) We have $H(X_i \searrow Y_i|Y_i) = (n-m)k$, $I(X_i;Y_i|X_i \wedge Y_i) = mk$, and $H(Y_i \searrow X_i|X_i) = \log \binom{n}{m}$. For $X = [X_1, \ldots, X_t]$ and $Y = [Y_1, \ldots, Y_t]$, we have $H(X \searrow Y|Y) = t(n-m)k$, $I(X;Y|X \wedge Y) = tmk$, and $H(Y \searrow X|X) = t \log \binom{n}{m}$. Now we can apply Theorem 3, and the statement follows. □

For the special case where $M = m = 1$, the obtained bounds are shown in Figure 1.

$t \geq \ldots$	$K \geq k$	$K < k$
$N \geq n$	$\frac{(N-1)K}{(n-1)k}$	$\max\left(\frac{(N-1)K}{(n-1)k}, \frac{\log N}{\log n}\right)$
$N < n$	$\frac{K}{k}$	1

Fig. 1. The bounds for $M = m = 1$.

4.2 Optimally Trading Message Length for Choice

We present a protocol allowing for increasing the number of messages sent in oblivious transfer if, at the same time, their length is reduced. The number of calls to the original oblivious transfer equals the lower bound of Theorem 4.

Let $n, k, t \in \mathbf{N}$, $t > 1$, $N = n^t$, and $K \leq k/n^{t-1}$. Protocol 1 reduces $\binom{N}{1}$-OT^K to t instances of $\binom{n}{1}$-OT^k.

Protocol 1. Let A's inputs be $x_0, \ldots, x_{N-1} \in \{0,1\}^K$, whereas B's choice is $c \in \{0, \ldots, N-1\}$. Let $c = \sum_{i=0}^{t-1} c_i n^i$, $c_i \in \{0, \ldots, n-1\}$.

1. A chooses $R_0^0, R_1^0, \ldots, R_{n-1}^0, R_0^1, \ldots, R_{n-1}^{t-1} \in_R \{0,1\}^k$.
2. A and B run $\binom{n}{1}$-OT^k t times. In round $i \in \{0, \ldots, t-1\}$, A inputs $R_0^i, \ldots, R_{n-1}^i$, and B inputs c_i. B receives Y_i.
3. A and B subdivide each string R_j^i and Y_i into n^{t-1} pieces of length $K = k/n^{t-1}$: $R_j^i = R_j^i(0)||\cdots||R_j^i(n^{t-1}-1)$, $Y_i = Y_i(0)||\cdots||Y_i(n^{t-1}-1)$.
4. For every $j \in \{0, \ldots, N-1\}$, let $j = \sum_{i=0}^{t-1} j_i n^i$ and $d_j = \sum_{i=0}^{t-2} (j_i + j_{t-1} \mod n) n^i$. A sends $m_j = x_j \oplus R_{j_0}^0(d_j) \oplus \cdots \oplus R_{j_{t-1}}^{t-1}(d_j)$ to B.
5. B calculates $d_c = \sum_{i=0}^{t-1} (c_i + c_{t-1} \mod n) n^i$ and outputs $y = m_c \oplus Y_0(d_c) \oplus \cdots \oplus Y_{t-1}(d_c)$.

Theorem 5. *Protocol 1 is a perfect reduction of $\binom{N}{1}$-OT^K to $\binom{n}{1}$-OT^k for $N = n^t$, $t > 1$, and $K \leq k/n^{t-1}$.*

Proof. If both players are honest, we have $Y_i = R_{c_i}^i$ for all $i \in \{0, \ldots, t-1\}$. Therefore,

$$\begin{aligned} y &= m_c \oplus Y_0(d_c) \oplus \cdots \oplus Y_{t-1}(d_c) \\ &= x_c \oplus m_c \oplus R_{c_0}^0(d_c) \oplus \cdots \oplus R_{c_{t-1}}^{t-1}(d_c) \oplus Y_0(d_c) \oplus \cdots \oplus Y_{t-1}(d_c) \\ &= x_c \ . \end{aligned}$$

A does not receive any messages, so she does not get any information about c.

It remains to be proven that B only gets information about one value sent by A, even if he is given all the other values. First of all, note that if two different j and j' take the same value d, then $j_i + j_{t-1} \equiv j'_i + j'_{t-1} \pmod n$ holds for all $i \in \{0, \ldots, t-1\}$. It follows $j_{t-1} \neq j'_{t-1}$, and, hence, $j_i \neq j'_i$ for all $i \in \{0, \ldots, t-1\}$. Therefore, every $R_j^i(d)$ is used at most once in Step 4. B has to choose a value c_i in every round, so he will always be able to reconstruct x_c for $c = \sum_{i=0}^{t} c_i n^i$. But for every other value $x_{c'}$, $c' \neq c$, he is missing at least one of the $R_{c'_i}^i(d_{c'})$ for $i \in \{0, \ldots, t-1\}$. This value is a one-time pad on $x_{c'}$ since it is not used anywhere else. Therefore, B does not get any information about any $x_{c'}$ for $c' \neq c$, even if he is given all the other values $x_{c''}$ for $c'' \neq c'$. □

5 Bit and String Commitment: Tight Lower Bounds

Unlike oblivious transfer, bit commitment that is *perfectly secure* for both parties is impossible to achieve even when they share correlated pieces of information

X and Y initially. Intuitively speaking, the reason is that if the commitment is perfectly hiding, there must exist, after the "commit message," an "open message" to be accepted by the receiver for any possible value one can commit to. Theorems 6 and 7 make this precise and explicit by giving lower bounds on the success probability of such cheating by the committer, depending on the distribution P_{XY}. Our bounds are improvements on similar bounds presented in [2] and [15].

Theorem 6. *Assume that a commitment protocol exists where the committer initially knows a random variable X and the receiver knows Y. If the protocol is perfectly hiding and the committer has committed to a value $v \in \mathcal{V}$, then the probability p_s that she succeeds in opening the commitment to a different value $v' \neq v$ is at least*

$$p_s \geq 2^{-H(Y \searrow X|X)} .$$

Proof. Note first that under the given assumptions, there must also exist a commitment protocol with the same security properties if the parties are given X and $Y \searrow X$, respectively, since the part of Y that is independent of X can be simulated by B because $X \longleftrightarrow Y \searrow X \longleftrightarrow Y$ is a Markov chain. As the protocol is perfectly hiding, there must exist, for every value v', an opening of the commitment to v' that B accepts. Let y' be the value maximizing $P_{Y|X=x}$. A then opens the commitment for v' in such a way that B accepts if his value y is equal to y', and this is successful if $y = y'$ indeed holds. The expected probability of this event is

$$\begin{aligned} E_X\left[2^{-H_\infty(Y \searrow X|X=x)}\right] &\geq 2^{-E_X[H_\infty(Y \searrow X|X=x)]} \\ &\geq 2^{-E_X[H(Y \searrow X|X=x)]} \\ &= 2^{-H(Y \searrow X|X)} . \end{aligned}$$

In the first step, we have used Jensen's inequality. □

Theorem 7. *Assume that a commitment protocol exists where the committer initially knows a random variable X and the receiver knows Y. If the protocol is perfectly hiding and the committer has committed to a value $v \in \mathcal{V}$, then the probability p_s that she succeeds in opening the commitment to a different value $v' \neq v$ is at least*

$$p_s \geq 2^{-H(X \searrow Y)+\log(|\mathcal{V}|-1)} .$$

Proof. We can assume without loss of generality that the pieces of information known to the parties are $X \searrow Y$ and Y. Let the committer hold x and commit to $v \in \mathcal{V}$, and let $v' \neq v$. Since the protocol is perfectly hiding, there must exist $x' \in \mathcal{X}$ such that the commit message sent corresponds to the correct commitment for v'. The probability of correctly guessing this value x', maximized over all v', is at least

$$2^{-H_\infty(X \searrow Y)}(|\mathcal{V}|-1) \geq 2^{-H(X \searrow Y)+\log(|\mathcal{V}|-1)} .$$

□

Corollary 2. *Assume that a commitment protocol exists where the committer initially knows a random variable X and the receiver knows Y. If the protocol is perfectly hiding and the committer has committed to a value $v \in \mathcal{V}$, then the probability p_s that she succeeds in opening the commitment to a different value $v' \neq v$ is at least*

$$p_s \geq \max\left(2^{-H(Y \searrow X|X)}\ ,\ 2^{-H(X \searrow Y)+\log(|\mathcal{V}|-1)}\right)\ .$$

The commitment protocol of [17] achieves this bound: Given a prime number q, we have $H(X \searrow Y) = 2\log q$, $H(Y \searrow X|X) = \log q$, and $|\mathcal{V}| = q$. It is perfectly hiding, and the "binding error probability" p_s is

$$p_s = 1/q = 2^{-H(Y \searrow X|X)}\ .$$

6 Concluding Remarks

We have presented three information-theoretic quantities with the property that no two-party protocol can increase them—so-called *monotones*. Based on these, we have derived new lower bounds on the possibility and efficiency of realizing oblivious transfer and bit commitment from pieces of correlated information, as well as on reductions between different versions of oblivious transfer. Finally, we have proposed a new protocol for such a reduction of the latter kind which is optimal.

We suggest as an open problem to find a general reduction of $\binom{N}{M}$-OT^K to $\binom{n}{m}$-OT^k which attains the given lower bound for *any* choice of the parameters. Furthermore, it would be interesting and useful to find similar monotones for *multi*-party protocols.

Acknowledgments

The authors thank Don Beaver, Claude Crépeau, Anderson Nascimento, and Renato Renner for interesting discussions on the subject of this paper, and three anonymous reviewers for their helpful comments on an earlier version. This work was supported by Canada's NSERC and Québec's FQRNT.

References

1. D. Beaver. Precomputing oblivious transfer. *Advances in Cryptology—Proceedings of CRYPTO '95*, LNCS, Vol. 963, pp. 97–109, Springer-Verlag, 1992.
2. C. Blundo, B. Masucci, D. R. Stinson, and R. Wei. Constructions and bounds for unconditionally secure non-interactive commitment schemes. *Designs, Codes, and Cryptography*, 26(1-3): 97–110, 2002.
3. G. Brassard, C. Crépeau, and S. Wolf. Oblivious transfers and privacy amplification. *Journal of Cryptology*, Vol. 16, No. 4, pp. 219–237, 2003.

4. N. J. Cerf, S. Massar, and S. Schneider. Multipartite classical and quantum secrecy monotones. *Phys. Rev. A*, Vol. 66, No. 042309, 2002.
5. C. Crépeau. *Correct and private reductions among oblivious transfers*. Ph. D. thesis, MIT, 1990.
6. C. Crépeau. Efficient cryptographic protocols based on noisy channels. *Advances in Cryptology—Proceedings of CRYPTO '97*, LNCS, Vol. 1233, pp. 306–317, Springer-Verlag, 1997.
7. C. Crépeau, K. Morozov, and S. Wolf. Efficient unconditional oblivious transfer from almost any noisy channel. *Proceedings of Fourth Conference on Security in Communication Networks (SCN) '04*, LNCS, Vol. 3352, pp. 47–59, Springer-Verlag, 2004.
8. C. Crépeau and M. Sántha. On the reversibility of oblivious transfer. *Advances in Cryptology—Proceedings of Eurocrypt '91*, LNCS, Vol. 547, pp. 106–113, Springer-Verlag, 1991.
9. Y. Dodis and S. Micali, Lower bounds for oblivious transfer reductions, *Advances in Cryptology—Proceedings of EUROCRYPT '99*, LNCS, Vol. 1592, pp. 42–55, Springer-Verlag, 1999.
10. M. Fitzi, S. Wolf, and J. Wullschleger. Pseudo-signatures, broadcast, and multi-party computation from correlated randomness. *Advances in Cryptology—Proceedings of CRYPTO '04*, LNCS, Vol. 3152, pp. 562–579, Springer-Verlag, 2004.
11. P. Gacs and J. Körner, Common information is far less than mutual information, *Probl. Contr. Inform. Theory*, Vol. 2, pp. 149–162, 1973.
12. H. Imai, J. Müller-Quade, A. Nascimento, and A. Winter. Rates for bit commitment and coin tossing from noisy correlation. *Proceedings of the IEEE International Symposium on Information Theory (ISIT '04)*, IEEE, 2004.
13. U. Maurer. Information-theoretic cryptography. *Advances in Cryptography—Proceedings of CRYPTO' 99*, LNCS, Vol. 1666, pp. 47–64, Springer-Verlag, 1999.
14. U. Maurer and S. Wolf. Unconditionally secure key agreement and the intrinsic conditional information. *IEEE Transactions on Information Theory*, Vol. 45, No. 2, pp. 499–514, 1999.
15. A.C.A. Nascimento, J. Müller-Quade, A. Otsuka, and H. Imai. Unconditionally secure homomorphic pre-distributed commitments. *Proceedings of AAECC 2003*, pp. 87–97, 2003.
16. R. Renner and S. Wolf. New bounds in secret-key agreement: the gap between formation and secrecy extraction. *Advances in Cryptography—Proceedings of EUROCRYPT 2003*, LNCS, Vol. 2656, pp. 562–577, Springer-Verlag, 2003.
17. R. L. Rivest. Unconditionally secure commitment and oblivious transfer schemes using private channels and a trusted initializer. Unpublished manuscript, 1999.
18. S. Wolf and J. Wullschleger. Zero-error information and applications in cryptography. *Proceedings of 2004 IEEE Information Theory Workshop (ITW 2004)*, 2004.
19. S. Wolf and J. Wullschleger. Oblivious transfer is symmetric. *Cryptology ePrint Archive*, Report 2004/336. `http://eprint.iacr.org/2004/336`, 2004.
20. S. Wolf and J. Wullschleger. Oblivious transfer and quantum non-locality. *Quantum Physics e-print Archive*, quant-ph/0502030, 2005.