Oblivious Transfer from Weak Noisy Channels

Jürg Wullschleger
University of Bristol, UK
j.wullschleger@bristol.ac.uk

September 30, 2008

Abstract

Various results show that oblivious transfer can be implemented using the assumption of *noisy channels*. Unfortunately, this assumption is not as weak as one might think, because in a cryptographic setting, these noisy channels must satisfy very strong security requirements.

Unfair noisy channels, introduced by Damgård, Kilian and Salvail [Eurocrypt '99], reduce these limitations: They give the adversary an unfair advantage over the honest player, and therefore weaken the security requirements on the noisy channel. However, this model still has many shortcomings: For example, the adversary's advantage is only allowed to have a very special form, and no error is allowed in the implementation.

In this paper we generalize the idea of unfair noisy channels. We introduce two new models of cryptographic noisy channels that we call the *weak erasure channel* and the *weak binary symmetric channel*, and show how they can be used to implement oblivious transfer. Our models are more general and use much weaker assumptions than unfair noisy channels, which makes implementation a more realistic prospect.

1 Introduction

Secure two-party computation, introduced in [Yao82], allows two mutually distrustful players to calculate a function in a secure way. This means that both players get the correct output, but nothing more than that. Even though secure two-party computation is generally impossible without any further assumption, it has been shown in [GV88, Kil88] that if a very simple primitive called *oblivious transfer* is available, then any two-party computation can be implemented in an unconditionally secure way.

Oblivious transfer was first defined in [Wie83], however without realizing its connection to cryptography. In the cryptographic context, the two variants of oblivious transfer were defined in [Rab81] and [EGL85], which were shown to be equally powerful in [Cré88]. Throughout this work, we will only consider *chosen one-out-of-two oblivious transfer*, or OT for short. Here, a sender can send two message bits x_0 and x_1, and a receiver can choose which of the two messages he wants to receive by sending a choice bit c. He receives x_c, but does not get to know the other message bit x_{1-c}, and the sender does not get to know the choice bit c. There exist various implementations of OT that are secure against computationally bounded adversaries, under various hardness assumptions. Against adversaries with unbounded computational power, OT can only be implemented if the players have access to an additional (weaker) functionality.

1.1 OT from (Unfair) Noisy Channels

In [CK88], it has been shown that OT can be implemented from various weaker forms of OT, as well as *noisy channels*. Therefore, noise is not always a bad thing; in a cryptographic context it can become a valuable resource. These protocols have later been improved and generalized in [Cré97], [CMW04] and [NW08]. The basic idea of all these protocol is very similar: First, they construct some kind of erasure channel. Then, this erasure channel is used many times to implement OT. The correctness and the security is guaranteed using error correcting codes and privacy amplification.

These noisy channels seem to be quite weak primitives and easily implementable, but they have some rather strong requirements: The statistics of the channel must be *exactly* the same in every instance, and know to both players. And, apart from the output of the channel, a dishonest players must not get *any* additional output.

In [DKS99], weaker forms of noisy channels called *unfair noisy channels* were introduced. Unfair noisy channels are binary symmetric noisy channels that let the dishonest player change the error-rate in the channel by a certain amount. For example, this makes the protocol secure against an adversary that might use better transmitters or detectors in order to break the protocol. In this model, OT must be implemented in a different way, using the following two steps. First, from only a few instances of the channel, a weak form of OT (called WOT) is constructed. In the second step, the security is amplified, i.e., many of these WOTs are used to get one secure instance of OT. The resulting protocol is only secure in the *semi-honest model*, i.e., under the assumption that the dishonest player follows the protocol. To make the protocol secure in the *malicious model*, where the dishonest player may deviate in an arbitrary way from the protocol, a third step is needed, which uses *bit commitments* and *zero-knowledge proofs* to force the dishonest player to follow the protocol.

The results from [DKS99] were later improved in [DFMS04], and OT amplification was improved in [Wul07].

1.2 Limitations of Unfair Noisy Channels

Even though unfair noisy channels are much weaker than (fair) noisy channels, they still have some very strong assumptions, which makes them hard to implement. Let us look at the following example:

A (fair) binary symmetric noisy channel with error ε lets a sender input a bit $x \in \{0,1\}$. The channel then outputs a values $Y \in \{0,1\}$ to the receiver, where $\Pr[Y \neq x] = \varepsilon$. Let us assume that neither the sender nor the receiver can influence ε, but that the dishonest receiver gets an additional value $E \in \{0,1\}$, where $\Pr[E = 1] = \mu$, and $E = 1 \Rightarrow Y = x$. Therefore, with some probability μ, the dishonest receiver gets to know that the value Y he received is in fact equal to x. If μ is small, then this channel is very close to a fair binary symmetric noisy channel. However, even then it cannot be modeled by an unfair noisy channel, because there, the receiver can never be sure that his received bit is the actual bit from the sender. Therefore, unfair noisy channels forbid the adversary to have this kind of advantage. In fact, they only allow the adversary *one, very special* advantage over the honest player.

Now, let us assume that we have implemented a noisy channel, and that the statistics of the channel show that the channel behaves like a fair noisy channel. What can we say about the channel? We certainly cannot conclude that the channel is really a fair noisy channel, as it might as well be the channel from the example above, with a small μ. And therefore, neither can the channel be modeled by an unfair noisy channel. To be able to implement OT in this situation, we need to have a model that allows the implementation to behave *arbitrarily* with some probability.

1.3 Contribution

The goal of this work is to present a new, more general and more realistic model for noisy channels (called *weak noisy channels*) and to show that oblivious transfer can be implemented in a unconditionally secure way, assuming that such weak noisy channels exist. The main difference of our model to the unfair noisy channel model is that we do not define a functionality for a weak noisy channel, but we merely state a list of conditions that weak noisy channels should satisfy. Therefore, weak noisy channels in fact cover a wide range of functionalities, and the reduction remains secure as long a functionality of this set is used. This makes our model much more realistic and easier to apply.

We will introduce the following three models of weak noisy channels:

- *Weak erasure channels in the semi-honest model*[1] *(PassiveWEC).* These are weak variants of erasure channels[2] (channels that transmit a bit with some probability).
- *Weak binary symmetric channels in the semi-honest model (PassiveWBSC).* As the unfair noisy channel, these are weak variants of binary symmetric channels.
- *Weak erasure channels in the malicious model (ActiveWEC).*

To show the flexibility and generality of our models, we show that it is very easy to implement a PassiveWEC from *gaussian channels*, and that the (passive) unfair noisy channel can be seen as an instance of a PassiveWBSC.

In Sections 3 to 5, we show the following reductions: PassiveWEC implies WOT, and PassiveWBSC implies PassiveWEC in the semi-honest model. Then, we show that ActiveWEC implies both bit commitment and a committed version of PassiveWEC. This implies that in a certain range of parameters, each of the three weak noisy channels allows for any secure two-party computation to be achieved. For each of the weak noisy channels, we also present a *simulation* of the channel using nothing else than noiseless communication, and in the case of ActiveWEC, shared randomness. Since it is impossible to implement bit commitment or oblivious transfer from noiseless communication and shared randomness, it is also impossible to implement them using the simulated weak noisy channels.

All proofs and some additional lemmas needed are in the appendix.

2 Preliminaries

In this section, we present some basic definitions and lemmas that we will need later.

We will use the following convention: Lower case letters will denote fixed values and upper case letters will denote random variables. Calligraphic letters will denote sets and domains of random variables. For a random variable X over $\mathcal{X}$, we denote its distribution by $P_X : \mathcal{X} \to [0,1]$ with $\sum_{x\in\mathcal{X}} P_X(x) = 1$. For a given distribution $P_{XY} : \mathcal{X} \times \mathcal{Y} \to [0,1]$, we write for the marginal distribution $P_X(x) := \sum_{y\in\mathcal{Y}} P_{XY}(x,y)$ and, if $P_Y(y) \neq 0$, $P_{X|Y}(x \mid y) := P_{XY}(x,y)/P_Y(y)$ for the conditional distribution. Let $h(x) := -x \log x - (1-x)\log(1-x)$ be the binary entropy function.

[1] See Section 2.2 for explanation of the semi-honest and the malicious model.

[2] Note that the original definition of OT by Rabin [Rab81] is in fact also an erasure channel, so a WEC is also a weak form of Rabin-OT.

2.1 Statistical Distance and Maximal Bit-Prediction Advantage

We will use the *statistical distance* and the *maximal bit-prediction advantage* to measure the weakness of our channels. Lemmas 1, 2 and 3 can easily be proven[3] and give some intuition about these measures: The random variable B (or C) indicates that an error occurred: If $B = 0$, everything is fine. But if $B = 1$, the adversary may have complete knowledge.

Definition 1. The *statistical distance* of two random variables X and Y (or two distributions P_X and P_Y) over the same domain $\mathcal{U}$ is defined as $\delta(P_X, P_Y) := \frac{1}{2}\sum_{u \in \mathcal{U}} |P_X(u) - P_Y(u)|$.

We say that X is ε-close to uniform with respect to Y, if $\delta(P_{XY}, P_U P_Y) \leq \varepsilon$, where P_U is the uniform distribution.

Lemma 1. *Let P_{BX} and P_{CY} be distributions over $\{0,1\} \times \mathcal{U}$ such that* $\Pr[B = 1] = \Pr[C = 1] = \varepsilon$. *Then $\delta(P_X, P_Y) \leq \varepsilon + (1-\varepsilon) \cdot \delta(P_{X|B=0}, P_{Y|C=0})$.*

Definition 2. Let P_{XY} be a distribution over $\{0,1\} \times \mathcal{Y}$. The *maximal bit-prediction advantage* of X from Y for a function f is defined as $\mathrm{PredAdv}(X \mid Y) := 2 \cdot \max_f \Pr[f(Y) = X] - 1$.

Lemma 2. *Let P_{XY} be any distribution over $\{0,1\} \times \mathcal{Y}$. There exists a conditional distribution $P_{B|XY}$ over $\{0,1\} \times \{0,1\} \times \mathcal{Y}$ such that* $\Pr[B = 1] \leq \mathrm{PredAdv}(X \mid Y)$ *and such that for all functions $f : \mathcal{Y} \to \{0,1\}$,* $\Pr[f(Y) = X \mid B = 0] = 1/2$.

Lemma 3. *Let P_{XY} be any distribution over $\{0,1\} \times \mathcal{Y}$ with $\delta(P_{Y|X=0}, P_{Y|X=1}) \leq \varepsilon$. There exists a random variable B over $\{0,1\}$ such that* $\Pr[B = 1 \mid X = 0] = \Pr[B = 1 \mid X = 1] = \varepsilon$, *and $P_{Y|X=0,B=0} = P_{Y|X=1,B=0}$.*

2.2 Adversaries

We distinguish between two different models, the *semi-honest model* and the *malicious model*. In the *semi-honest model*, the adversary is *passive*, which means that she follows the protocol, but may try to get additional knowledge from the messages received. In the malicious model, the adversary *active*, which means that he may change his behavior in an arbitrary way.

2.3 Oblivious Transfer Amplification

Our work is based on *oblivious transfer amplification* from [DKS99, Wul07], which gives a way to implement oblivious transfer (OT) from weak oblivious transfer (WOT). We will take the definition of WOT from the full version of [Wul07], however we use the weaker requirement of $\mathrm{PredAdv}(C \mid U) \leq p$ instead of $\mathrm{PredAdv}(C \mid U, E) \leq p$. As explained there, the reduction of OT to WOT still works for this weaker definition, as long as the error correction is always done from the sender to the receiver, which is normally the case.

Definition 3 (Weak oblivious transfer, semi-honest model)**.** A *weak (randomized) oblivious transfer*, denoted by (p, q, ε)-WOT, is a primitive between a sender and a receiver, that outputs (X_0, X_1) to the honest sender and (C, Y) to the honest receiver. Let U be the additional, auxiliary output[4] to a dishonest sender and let V be the auxiliary output to a dishonest receiver. Let $E := X_C \oplus Y$. The following conditions must be satisfied:

- *Correctness:* $\Pr[E = 1] \leq \varepsilon$.
- *Receiver Security:* $\mathrm{PredAdv}(C \mid U) \leq p$.

[3] For proofs of Lemmas 1 and 2, see for example [Wul07] and [Hol06]. A proof of Lemma 3 is in the appendix.

[4] Or the *view* of the adversary, i.e., everything he knows at the end of the protocol.

- *Sender Security:* $\mathrm{PredAdv}(X_{1-C} \mid V, E) \leq q$.

Theorem 1 ([Wul07])**.** *Let p, q and ε be constants such at least one of the following conditions holds:*

$$p+q+2\varepsilon \leq 0.24 \;, \quad 22q+44\varepsilon < 1-p \;, \quad 22p+44\varepsilon < 1-q \;, \quad 49p+49q < (1-2\varepsilon)^2 \;,$$

$$q=0 \;\wedge\; p<(1-2\varepsilon)^2 \;, \qquad p=0 \;\wedge\; q<(1-2\varepsilon)^2 \;, \qquad \varepsilon=0 \;\wedge\; p+q<1 \;.$$

Then there exist a protocol that efficiently implements OT from (p,q,ε)-WOT secure in the semi-honest model.

2.4 Bit Commitment

To achieve oblivious transfer in the malicious model, we will need *bit commitments.* A bit commitment scheme is a pair of protocols, a **Commit** protocol and a **Open** protocol, executed between a commiter and a receiver. The players first execute the Commit protocol, where the commiter has an input b. Then, they may also execute the Open protocol. After the Open protocol, the receiver either accepts or rejects. If he accepts, he gets a value b'. The protocols are ε-secure, if they satisfy the following properties:

- *Correctness*: If both players follow the protocols, then the receiver rejects with a probability smaller than ε, and if he accepts, he outputs $b' = b$ with probability at least $1-\varepsilon$.
- *Binding*: If the receiver is honest, then for any malicious sender, with probability $1-\varepsilon$, there exists at most one value after the commit protocol that the receiver will accept with a probability bigger than ε in the open phase.
- *Hiding*: If commiter is honest, then no malicious receiver gets to know b with a probability bigger than ε.

3 Weak Erasure Channel in the Semi-Honest Model

In this section, we present a reduction of *weak erasure channels (WEC)* to WOT in the semi-honest model.

A weak erasure channel lets a honest sender send a bit, which is then received by the honest receiver with a certain probability, and gets lost otherwise. Dishonest players are allowed to receive some additional information, so a dishonest receiver may get to know some information about the input even in the case where the channel lost the bit, and a dishonest sender may get information about whether the bit has been lost or not. Note that our definition is randomized, i.e., the honest sender cannot choose his input, it is chosen by the channel.

Definition 4 (Weak Erasure Channel in the Semi-Honest Model)**.** $(d_0, d_1, p, q, \varepsilon)$-$\mathsf{PassiveWEC}$ is a primitive where the honest sender has output $X \in \{0,1\}$ and the honest receiver has output $Y \in \{0,1,\Delta\}$. Furthermore, the dishonest sender may receive an additional value U, and the dishonest receiver may receive an additional value V. These values must satisfy the following conditions:

- *Correctness:* $\Pr[Y = \Delta] \in [d_0, d_1]$, $\Pr[Y \neq X \mid Y \neq \Delta] \leq \varepsilon$.
- *Receiver Security:* $\delta(P_{XU|Y\neq\Delta}, P_{XU|Y=\Delta}) \leq p$.

- *Sender Security:* $\mathrm{PredAdv}(X \mid V, Y = \Delta) \leq q$.

The parameters can be interpreted as follows: d_0,d_1 and ε are parameters of the honest players. The probability that the output of the channel is Δ is in the interval $[d_0, d_1]$. (Defining this as an interval gives some freedom to the implementation, which may be important, as parameters often cannot be known precisely[5].) ε is the probability that the output of the honest receiver is wrong, if the output is not Δ. According to Lemma 2, q is the probability that the dishonest receiver gets to know the input of the channel, given that the output of the channel is Δ, and according to Lemma 3, p is the probability that a dishonest sender gets to know whether $Y = \Delta$ or $Y \neq \Delta$.

3.1 Simulation of PassiveWEC

We start by showing for which values a PassiveWEC can be simulated by only using noiseless communication. Since OT cannot be implemented from noiseless communication, such PassiveWEC therefore cannot be used to implement OT, as well. In the following simulation, we require that $d, g \in [0, 1]$, and $g \geq (1 - 2\varepsilon)(1 - d)$.

Protocol SimWEC(d, ε, g)

1. The sender chooses x uniformly at random. He sends the receiver $m := x$ probability g, and and $m := \Delta$ otherwise. She outputs x.
2. If the receiver get $m \in \{0, 1\}$, he outputs $y := m$ with probability $\frac{(1-2\varepsilon)(1-d)}{g}$, and $y := \Delta$ otherwise.
3. If the receiver get $m = \Delta$, he outputs y chosen at random with probability $\frac{2\varepsilon(1-d)}{1-g}$, and $y := \Delta$ otherwise.

Theorem 2. *For any d, ε, p and q, where $p+q+2\varepsilon \geq 1$, $(d, d, \varepsilon, p, q)$-PassiveWEC is simulatable in the semi-honest model.*

3.2 WOT from PassiveWEC

Protocol PassiveWECtoWOT

1. The sender and the receiver execute PassiveWEC twice. The sender receives (x_0, x_1), the receiver (y_0, y_1).
2. If there exists a c, such that $y_c \neq \Delta$ and $y_{1-c} = \Delta$, then the receiver sets $y := y_c$, outputs (c, y), tells the sender to terminate the protocol and terminates.
3. If the sender receives the message to terminate the protocol, he outputs (x_0, x_1) and terminates. Otherwise, they restart the protocol.

Theorem 3. *Protocol PassiveWECtoWOT securely implements a*

$$\left(1 - \frac{2d_0(1-d_1)}{d_1(1-d_0) + d_0(1-d_1)}(1-p)^2, q, \varepsilon\right)\text{-WOT}$$

secure against passive adversaries out of $(d_0, d_1, p, q, \varepsilon)$-PassiveWEC. The expected number of instances of WEC that this protocol uses is at most $1/\min(2d_0(1-d_0), 2d_1(1-d_1))$.

[5] This will be useful in Protocol ActiveToPassiveWEC.

3.3 An Example: The Gaussian Channel

The *gaussian channel* is often used in information theory as a model of a noisy channel, because it is quite close to a real channel. It has been shown that a perfect and fair gaussian channel implies bit commitment, see [NSBI07, OM08]. A gaussian channel is a channel where the sender has input $x_g \in \mathbb{R}$ and the receiver has output $Y_g = x_g + E_g$, where $E_g \sim \mathcal{N}(0,1)$, i.e., the channel has an additive error that is normal distributed.

We can easily implement a PassiveWEC from this channel in the following way: Let $a, b \in \mathbb{R}^+$. The sender chooses $x \in \{0,1\}$ uniformly at random, sends $x_g := (2x-1)a$ and outputs x. The receiver gets y_g, and outputs $y = \delta$ if $|y_g| \leq b$, $y = 1$ if $y_g > b$ and $y = 0$ otherwise. With an arbitrary small error, we can make the gaussian channel discrete. In the limit, we get a $(\varepsilon, d, d, p, q)$-PassiveWEC, where $d = \Phi(b-a) - \Phi(-a-b)$, $\varepsilon = \frac{\Phi(-a-b)}{1-\Phi(b-a)+\Phi(-a-b)}$, $p = 0$ and $q = \Phi(b-a) - \Phi(-a) - \Phi(-a) + \Phi(-a-b)$. Choosing for example $a = 1$ and $b = 2$, we get $d \approx 0.8427$, $\varepsilon \leq 0.009$, and $q \leq 0.526$. Theorem 3 tells us that this implies $(0, 0.526, 0.009)$-WOT. Since $22 \cdot 0 + 44 \cdot 0.009 < 1 - 0.526$, it follows from Theorem 1 that oblivious transfer can be implemented. Together with the bit commitment protocols from [NSBI07, OM08], this implies (using a protocol similar to ActiveToPassiveWEC) that OT can be implemented from (perfect and fair) gaussian channels in the malicious model.

Note that in contrast to the reductions from [NSBI07, OM08], this reduction also works for gaussian channels that are neither perfect nor fair.

4 Weak Binary Symmetric Channel in the Semi-Honest Model

Weak Binary Symmetric Channel is a weak form of a binary symmetric channel. The channel transmits the input bit of the sender to the receiver, but flips the bit with some probability. And the dishonest players may get to know with some probability if the bit was flipped or not. Again, the definition is randomized.

Definition 5 (Weak Binary Symmetric Channel in the Semi-Honest Model)**.** The primitive $(\varepsilon, \varepsilon_0, \varepsilon_1, p, q)$-PassiveWBSC is defined as follows: The honest sender has output $X \in \{0,1\}$ and the honest receiver has output $Y \in \{0,1\}$. Furthermore, the dishonest sender may receive an additional value $U \in \mathcal{U}$, and the dishonest receiver may receive an additional value $V \in \mathcal{V}$. These values must satisfy the following conditions:

- *Correctness:* $\Pr[X = 0] \in [\frac{1-\varepsilon}{2}, \frac{1+\varepsilon}{2}]$, and for $x \in \{0,1\}$, $\Pr[Y \neq x] \in [\varepsilon_0, \varepsilon_1]$.
- *Receiver Security:* $\delta(P_{UX|Y=X}, P_{UX|Y\neq X}) \leq p$.
- *Sender Security:* For all $y \in \{0,1\}$: $\delta(P_{V|X=0,Y=y}, P_{V|X=1,Y=y}) \leq q$.

The parameters can be interpreted as follows: ε is the bias of X, and ε_0 and ε_1 define the error interval of the honest players. From Lemma 3 follows that p is the probability that the sender, and q is the probability that the receiver gets to know whether $X = Y$ or not. However, in order to make our reduction work, the sender security has a slightly different form than the receiver security. Note that if $\varepsilon = 0$ and $\varepsilon_0 = \varepsilon_1$, the sender security implies $\delta(P_{VY|Y=X}, P_{VY|Y\neq X}) \leq q$. So in this case, the sender security is strictly stronger than the receiver security.

4.1 Simulation of PassiveWBSC

The following simulation is basically the same as in [DKS99]. Let $\varepsilon_A, \varepsilon_B \in [0, \frac{1}{2}]$.

Protocol SimWBSC$(\varepsilon_A, \varepsilon_B)$

1. The players toss a uniform coin $M \in \{0,1\}$.
2. The sender calculates $X := 1-M$ with probability ε_A and $X := M$ otherwise, and outputs X.
3. The receiver calculates $Y := 1-M$ with probability ε_B and $Y := M$ otherwise, and outputs Y.

Theorem 4. *The Protocol $\mathsf{SimWBSC}(\varepsilon_A, \varepsilon_B)$ securely implements a $(0, \varepsilon, \varepsilon, p, q)$-PassiveWBSC in the semi-honest model for $\varepsilon := \varepsilon_A(1-\varepsilon_B) + \varepsilon_B(1-\varepsilon_A)$, $p := \frac{(1-\varepsilon_A)(1-\varepsilon_B)}{1-\varepsilon} - \frac{\varepsilon_A(1-\varepsilon_B)}{\varepsilon}$, and $q := \frac{(1-\varepsilon_A)(1-\varepsilon_B)}{1-\varepsilon} - \frac{(1-\varepsilon_A)\varepsilon_B}{\varepsilon}$.*

Theorem 4 implies that $(0, \varepsilon, \varepsilon, p, q)$-PassiveWBSC is simulatable if $p + q > 1$.

4.2 PassiveWEC from PassiveWBSC

We will now give a reduction of PassiveWEC to PassiveWBSC. The protocol itself has already been used in [CK88] and [Cré97]. The intuition behind the following protocol is simple: The sender sends a bit twice over a binary noisy channel. If the receiver gets twice the same message, he can guess quite accurately what the sender has sent and output that. If he receives two different messages, he cannot guess the senders input and outputs a Δ. Note that since we use randomized primitives, the sender cannot choose her input, and therefore has to additionally send $x_0 \oplus x_1$.

Protocol PassiveWBSCtoWEC

1. The players execute PassiveWBSC twice. The sender gets (x_0, x_1), the receiver (y_0, y_1).
2. The sender sends $k := x_0 \oplus x_1$ to the receiver and outputs $x := x_0$.
3. If $y_0 \oplus y_1 = k$, the receiver outputs $y := y_0$. Otherwise, he outputs $y := \Delta$.

Theorem 5. *Let*

$$\begin{aligned} d_0 &:= \min(2\varepsilon_0(1-\varepsilon_0), 2\varepsilon_1(1-\varepsilon_1)) , \\ d_1 &:= \max(2\varepsilon_0(1-\varepsilon_0), 2\varepsilon_1(1-\varepsilon_1), \varepsilon_0(1-\varepsilon_1) + \varepsilon_1(1-\varepsilon_0)) . \end{aligned}$$

Protocol PassiveWBSCtoWEC securely implements a

$$\left(d_0, d_1, 1-(1-p)^2, 1 - \left(1 - \frac{\varepsilon_1 - \varepsilon_0}{\varepsilon_1 + \varepsilon_0 - 2\varepsilon_0\varepsilon_1} - \frac{2\varepsilon}{1+\varepsilon^2}\right)(1-q)^2, \frac{\varepsilon_1^2}{\varepsilon_1^2 + (1-\varepsilon_1)^2}\right)\text{-PassiveWEC}$$

in the semi-honest model out of two independent instances of $(\varepsilon, \varepsilon_0, \varepsilon_1, p, q)$-PassiveWBSC.

4.3 An Example: The Unfair Noisy Channel

The *passive unfair noisy channel* (δ, γ)-PassiveUNC[6] from [DKS99, DFMS04] is a special case of a PassiveWBSC, namely a $(0, \delta, \delta, p, p)$-PassiveWBSC, where

$$p := \frac{(1-\delta)\delta - (1-\gamma)\gamma}{(1-2\gamma)\delta(1-\delta)} .$$

[6] The exact definition is given in the appendix.

5 WEC in the Malicious Model

The assumption that the adversary is semi-honest and therefore follows the protocol is quite strong and often too strong. As shown in [GMW87], there exist compilers that can convert protocols which are only secure in the semi-honest model into protocols that are also secure in the malicious model. The basic idea is that at the beginning, the players are committed to all the secret data they have, and after every computation step they do, they commit to the newly computed values and show with a zero-knowledge proof that the new committed value contains indeed the correct value, according to the protocol. (See [DFMS04] for a more detailed discussion.) To implement this in our setting, we need two things: A bit commitment protocol, and a protocol that implements a committed version of the passive weak noisy channel. Here, we will concentrate on the WEC. (We did not include the WBSC because we were not able to come up with a similar simple definition for WBSC in the malicious model as for WEC.)

We will define ActiveWEC, which is a WEC in the malicious model, and show that it implies both, bit commitment and a committed version of PassiveWEC. In the malicious model, the dishonest player may choose an attack where he does not get the output of the honest player. Therefore, the security conditions have to be stated in a different way.

Definition 6 (Weak Erasure Channel in the Malicious Model)**.** $(d_0, d_1, p, g, \varepsilon)$-ActiveWEC is a primitive with the following properties.

- *Correctness:* If both players are honest, then the sender has output $X \in \{0, 1\}$ and the receiver has output $Y \in \{0, 1, \Delta\}$, where $\Pr[Y = \Delta] \in [d_0, d_1]$ and $\Pr[Y \neq X \mid Y \neq \Delta] \leq \varepsilon$.
- *Receiver Security:* If the receiver is honest, then for all dishonest sender with auxiliary input z and output U, the receiver has output $Y \in \{0, 1, \Delta\}$ where $\Pr[Y = \Delta] \in [d_0, d_1]$ and $\delta(P_{U|Z=z,Y\neq\Delta}, P_{U|Z=z,Y=\Delta}) \leq p$.
- *Sender Security:* If the sender is honest, then for all dishonest receiver with auxiliary input z and output V, the sender has output $X \in \{0, 1\}$ and $\mathrm{PredAdv}(X \mid V, Z = z) \leq g$.

Note that also the honest receiver can guess X using $f(Y) := Y$ if $Y \neq \Delta$, and either 0 or 1 if $Y = \Delta$. We get

$$\Pr[f(Y) = X] \geq d_1/2 + (1 - \varepsilon)(1 - d_1) \ ,$$

and hence

$$\mathrm{PredAdv}(X \mid Y) \geq d_1 + 2(1 - \varepsilon)(1 - d_1) - 1 = (1 - 2\varepsilon)(1 - d_1) \ .$$

Therefore, a ActiveWEC can only be implemented if $g \geq (1 - 2\varepsilon)(1 - d_1)$.

5.1 Simulation

Using the same simulation as for the semi-honest case, we get

Theorem 6. *For any d, ε, p and q, where*

$$dp + g + 2\varepsilon \geq 1 \qquad \wedge \qquad g \geq (1 - 2\varepsilon)(1 - d) \ ,$$

$(d, d, \varepsilon, p, g)$-ActiveWEC is simulatable in the malicious model, given that the players have access to a source of trusted shared randomness.

5.2 Bit Commitment

Our commitment protocol takes parameters n, c, m and ℓ, where n is the number of instances used, c the error-tolerance of the protocol, ℓ the number of bits committed to. κ is the error. Let $c := n^{-1/3}$, and $\kappa := \exp(-2(1-d_1-c)nc^2)$. Let b be the maximum value that that satisfies

$$(1-d) \cdot b - \sqrt{\frac{b}{2} \cdot \ln \frac{1}{\kappa}} \leq (\varepsilon + c)(1-d)n$$

for all $d \in [d_0 - c, d_1 + c]$. Let

$$m := (d_1 p + c)n + 2b + 1$$

and let $\mathcal{C} \subset \{0,1\}^n$ be a (n,k,m)-linear code[7], i.e., with 2^k elements and minimal distance m. Let

$$\ell := k - (g+c) \cdot n - 3\log(1/\kappa) \; .$$

We also require that n is big enough such that $\ell > 0$. Let H be the parity-check matrix of $\mathcal{C}$ and $g : \mathcal{R} \times \{0,1\}^n \to \{0,1\}^\ell$ be two 2-universal hash function. In the following protocol, the sender is the commiter.

Protocol $\mathsf{ActiveWECtoBC}$

Commit(b).

- The parties execute $\mathsf{ActiveWEC}$ n times. The sender gets values $x = (x_0, \ldots, x_{n-1})$, and the receiver gets $y = (y_0, \ldots, y_{n-1})$.
- The commiter chooses $r \in \mathcal{R}$ uniformly at random and sends it to the receiver.
- The commiter sends $s := (H(x), b \oplus g(r,x))$ to the receiver.

Open.

- The commiter sends (b, x) to the receiver.
- Let n_Δ be the number of y_i equal to Δ. The receiver checks that $n_\Delta / n \in [d_0 - c, d_1 + c]$ and that the number i where $y_i \neq x_i$ and $y_i \neq \Delta$ is smaller than $(n - n_\Delta)(\varepsilon + c)$. He also checks that $s = (H(x), b \oplus g(r,x))$. If this is the case, he accepts, and rejects otherwise.

In the protocol, the commiter has to send the receiver the parity-check of a code, because then the commiter cannot guess with non-negligible probability more than one value x that passes the test of the receiver in the open phase. The commiter extracts a string of size ℓ from x, where ℓ is chosen small enough such that the receiver has almost no information about it.

Theorem 7. *Protocol $\mathsf{ActiveWECtoBC}$ implements a commitment with an error of 4κ, out of n instances of $(d_0, d_1, p, g, \varepsilon)$-$\mathsf{ActiveWEC}$.*

If

$$k \leq \left(1 - h\left(\frac{m}{n}\right)\right) n - s$$

a random linear (n,k)-code has a minimal distance of at least m with probability at least $1 - 2^{-s}$. If we choose a random linear code and let $n \to \infty$, then $b/n \to \varepsilon$, and hence $m/n \to d_1 p + 2\varepsilon$. From the property of the random linear code, we get $k/n \to 1 - h(d_1 p + 2\varepsilon)$. We need $\ell > 0$, which is equivalent to $g < k/n$. We get the following corollary.

[7] Since we do not have to decode $\mathcal{C}$, this could be a random linear code.

Corollary 1. *For any d_0, d_1, ε, p and q where*

$$d_1 p + 2\varepsilon < \frac{1}{2}, \qquad \text{and} \qquad g + h(d_1 p + 2\varepsilon) < 1 \ ,$$

we can implement a bit commitment from $(d_0, d_1, p, g, \varepsilon)$-ActiveWEC.

Our bound optimal for $p = 0 \wedge \varepsilon = 0$. Otherwise, it does not reach the simulation bound, since $h(x) > x$ for all $0 < x < \frac{1}{2}$. It would be interesting to know whether this bound can be improved.

A commitment in the other direction (where the receiver is the commiter) seems to be impossible: The only secret the receiver has is the information whether $Y = \Delta$ or not. But this information is generally not correlated with X, and hence the honest sender cannot verify it. Therefore, in order to be able to implement bit commitment in both directions, the parties are required to have an ActiveWEC in both directions.

5.3 Committed PassiveWEC from ActiveWEC

In the following, we present the protocol to implement a committed version of PassiveWEC in the malicious model, using ActiveWEC. It uses a similar idea already used in [DFMS04]: The players execute ActiveWEC n times and commit to their output values. Then, they open all except one randomly chosen one, and check if the statistics are fine. If they are, then with high probability, also the statistics of the remaining instance is fine.

The following lemma is essential to the proof, because it can be used to bound the parameter p for any committed value Y produced by the dishonest receiver, if he passes the test by the honest sender.

Lemma 4. *Let P_{XV} be a distribution over $\{0,1\} \times \mathcal{V}$. If $\mathrm{PredAdv}(X \mid V) \leq g$, then for any function $Y = f(V) \in \{0, 1, \Delta\}$ where $\Pr[Y = \Delta] \in [d_0, d_1]$ and $\Pr[Y \neq X \mid Y \neq \Delta] \leq \varepsilon$, we have*

$$\delta(P_{V|X=0,Y=\Delta}, P_{V|X=1,Y=\Delta}) \leq \frac{g - (1 - 2\varepsilon)(1 - d_1)}{d_1} \ .$$

In addition to ActiveWEC, our protocol needs bit commitments and coin-tosses. Coin-toss can easily be implemented using bit commitments.

Again, c is the error-tolerance, and κ is the error in the protocol. We choose $c := n^{-1/3}$ and $\kappa := \exp(-2(1 - d_1 - c)nc^2)$. Furthermore, let n be big enough such that $c \geq 1/((1 - d_1 - c)n)$.

Protocol ActiveToPassiveWEC

1. The sender and the receiver execute ActiveWEC n times. The sender gets $(x_0, \ldots, x_{n-1})$, and the receiver $(y_0, \ldots, y_{n-1})$.

2. Both players commit to their values.

3. Using coin-toss, they randomly select one instance s of the n instances.

4. They open all commitments, except for instance s. If any of the players does not accept one opening of a commitment, they abort.

5. Let n_Δ be the number of y_i that is equal to Δ. They check if n_Δ is in the interval $[(d_0 - c) \cdot n - 1, (d_1 + c) \cdot n]$, and the number of y_i that is not equal to Δ nor x_i is smaller than $(\varepsilon + c) \cdot (n - n_\Delta)$. If not, they abort.

6. The sender outputs $x := x_s$, the receiver $y := y_s$.

Theorem 8. *Protocol ActiveToPassiveWEC implements a committed version of*

$$\left(d_0 - 2c, d_1 + 2c, p, \frac{g - (1-2\varepsilon)(1-d_1)}{d_1} + \frac{4}{d_1^2}c, \varepsilon + 2c\right)\text{-}\mathsf{PassiveWEC}$$

with an error of at most 3κ in the malicious model. It uses coin-toss, bit commitment in both directions and n independent instances of $(d_0, d_1, p, g, \varepsilon)$-ActiveWEC.

Note that c is just polynomially small, and it cannot be made negligible. Here we see an advantage of our definition compared to the PassiveUNC in [DKS99, DFMS04]: We do not have to introduce the additional error parameter $p(k)$ as it has to be done for the committed version of the PassiveUNC, nor do we have to add an additional amplification step to the reduction to make this additional error negligible.

Acknowledgment

I was supported by the U.K. EPSRC, grant EP/E04297X/1.

References

[BBR88] C. H. Bennett, G. Brassard, and J.-M. Robert. Privacy amplification by public discussion. *SIAM Journal on Computing*, 17(2):210–229, 1988.

[Cac97] C. Cachin. Smooth entropy and rényi entropy. In *Advances in Cryptology — EUROCRYPT '97*, volume 1233 of *LNCS*, pages 193–208. Springer-Verlag, 1997.

[CK88] C. Crépeau and J. Kilian. Achieving oblivious transfer using weakened security assumptions (extended abstract). In *Proceedings of the 29th Annual IEEE Symposium on Foundations of Computer Science (FOCS '88)*, pages 42–52, 1988.

[CMW04] C. Crépeau, K. Morozov, and S. Wolf. Efficient unconditional oblivious transfer from almost any noisy channel. In *Proceedings of Fourth Conference on Security in Communication Networks (SCN)*, volume 3352 of *LNCS*, pages 47–59. Springer-Verlag, 2004.

[Cré88] C. Crépeau. Equivalence between two flavours of oblivious transfers. In *Advances in Cryptology — EUROCRYPT 1987*, LNCS, pages 350–354. Springer-Verlag, 1988.

[Cré97] C. Crépeau. Efficient cryptographic protocols based on noisy channels. In *Advances in Cryptology — CRYPTO '97*, volume 1233 of *LNCS*, pages 306–317. Springer-Verlag, 1997.

[DFMS04] I. Damgård, S. Fehr, K. Morozov, and L. Salvail. Unfair noisy channels and oblivious transfer. In *Theory of Cryptography Conference — TCC '04*, volume 2951 of *LNCS*, pages 355–373. Springer-Verlag, 2004.

[DKS99] 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 — EUROCRYPT '99*, volume 1592 of *LNCS*, pages 56–73. Springer-Verlag, 1999.

[EGL85] S. Even, O. Goldreich, and A. Lempel. A randomized protocol for signing contracts. *Commun. ACM*, 28(6):637–647, 1985.

[GMW87] O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game. In *Proceedings of the 21st Annual ACM Symposium on Theory of Computing (STOC '87)*, pages 218–229. ACM Press, 1987.

[GV88] O. Goldreich and R. Vainish. How to solve any protocol problem - an efficiency improvement. In *Advances in Cryptology — CRYPTO '87*, LNCS, pages 73–86. Springer-Verlag, 1988.

[Hol06] T. Holenstein. *Strengthening key agreement using hard-core sets.* PhD thesis, ETH Zurich, Switzerland, 2006. Reprint as vol. 7 of *ETH Series in Information Security and Cryptography*, Hartung-Gorre Verlag.

[ILL89] R. Impagliazzo, L. A. Levin, and M. Luby. Pseudo-random generation from one-way functions. In *Proceedings of the 21st Annual ACM Symposium on Theory of Computing (STOC '89)*, pages 12–24. ACM Press, 1989.

[Kil88] J. Kilian. Founding cryptography on oblivious transfer. In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing (STOC '88)*, pages 20–31. ACM Press, 1988.

[MW97] U. Maurer and S. Wolf. Privacy amplification secure against active adversaries. In *Advances in Cryptology — CRYPTO '97*, volume 1294 of *LNCS*, pages 307–321. Springer-Verlag, 1997.

[NSBI07] A.C.A. Nascimento, S. Skludarek, J. Barros, and H. Imai. The commitment capacity of the gaussian channel is infinite. *IEEE Trans. on Information Theory, Special Issue on Information Security*, 2007.

[NW08] A. Nascimento and A. Winter. On the oblivious transfer capacity of noisy correlations. *IEEE Trans. on Information Theory*, 54(6), 2008.

[OM08] F. Oggier and K. Morozov. A practical scheme for string commitment based on the gaussian channel. In *Proceedings of 2006 IEEE Information Theory Workshop (ITW '08)*, 2008.

[Rab81] M. O. Rabin. How to exchange secrets by oblivious transfer. Technical Report TR-81, Harvard Aiken Computation Laboratory, 1981.

[RW05] R. Renner and S. Wolf. Simple and tight bounds for information reconciliation and privacy amplification. In *Advances in Cryptology — ASIACRYPT 2005*, volume 3788 of *LNCS*, pages 199–216. Springer-Verlag, 2005.

[Wie83] S. Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983.

[Wul07] J. Wullschleger. Oblivious-transfer amplification. In *Advances in Cryptology — EUROCRYPT '07*, LNCS. Springer-Verlag, 2007. Full version (PhD Thesis, ETH Zurich) available at http://arxiv.org/abs/cs.CR/0608076.

[Yao82] A. C. Yao. Protocols for secure computations. In *Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science (FOCS '82)*, pages 160–164, 1982.

A Appendix

A.1 Proofs of Section 2

Proof of Lemma 3. We define B as

$$P_{B|XY}(0 \mid x,y) := \frac{\min(P_{Y|X}(y \mid 0), P_{Y|X}(y \mid 1))}{P_{Y|X}(y \mid x)} \ .$$

For $x \in \{0,1\}$, we get

$$\begin{aligned}
\Pr[B = 1 \mid X = x] &= \sum_y P_{Y|X}(y \mid x) P_{B|XY}(1 \mid x, y) \\
&= \sum_y P_{Y|X}(y \mid x) \left(1 - \frac{\min(P_{Y|X}(y \mid 0), P_{Y|X}(y \mid 1))}{P_{Y|X}(y \mid x)}\right) \\
&= \sum_y \big(P_{Y|X}(y \mid x) - \min(P_{Y|X}(y \mid 0), P_{Y|X}(y \mid 1))\big) \\
&= \delta(P_{Y|X=0}, P_{Y|X=1}) \ .
\end{aligned}$$

For all y, we have

$$\begin{aligned}
\Pr[Y = y \mid X = 0, B = 0] &= \frac{\Pr[Y = y \mid X = 0] \cdot \Pr[B = 0 \mid X = 0, Y = y]}{\Pr[B = 0 \mid X = 0]} \\
&= \frac{\min(P_{Y|X}(y \mid 0), P_{Y|X}(y \mid 1))}{\Pr[B = 0 \mid X = 0]} \\
&= \frac{\min(P_{Y|X}(y \mid 0), P_{Y|X}(y \mid 1))}{\Pr[B = 0 \mid X = 1]} \\
&= \Pr[Y = y \mid X = 1, B = 0]
\end{aligned}$$

Finally, if $\delta(P_{Y|X=0}, P_{Y|X=1}) < \varepsilon$, we can additionally increase $\Pr[B = 1 \mid X = x]$, without violating the condition. □

We will also need the following two lemmas for the maximal bit-prediction advantage.

Lemma 5. *Let P_{BXY} be any distribution over $\{0,1\} \times \{0,1\} \times \mathcal{Y}$. We have*

$$\mathrm{PredAdv}(X \mid Y) \leq \Pr[B = 0] \cdot \mathrm{PredAdv}(X \mid Y, B = 0) + \Pr[B = 1] \cdot \mathrm{PredAdv}(X \mid Y, B = 1) \ .$$

Proof. Let f be a function that maximizes $\mathrm{PredAdv}(X \mid Y)$. We have

$$\begin{aligned}
\mathrm{PredAdv}(X \mid Y) &= \Pr[B = 0] \cdot (2 \cdot \Pr[f(Y) = X \mid B = 0] - 1) \\
&\quad + \Pr[B = 1] \cdot (2 \cdot \Pr[f(Y) = X \mid B = 1] - 1) \\
&\leq \Pr[B = 0] \cdot \mathrm{PredAdv}(X \mid Y, B = 0) + \Pr[B = 1] \cdot \mathrm{PredAdv}(X \mid Y, B = 1) \ .
\end{aligned}$$

□

Lemma 6. *Let P_{XY} be a distribution over $\{0,1\} \times \mathcal{Y}$, where $\delta(P_{Y|X=0}, P_{Y|X=1}) \leq b$ and* $\mathrm{PredAdv}(X) \leq a$. *Then* $\mathrm{PredAdv}(X \mid Y) \leq 1 - (1 - a)(1 - b)$.

Proof. We can apply Lemma 3, which defines a random variable B such that

$$\Pr[B = 1 \mid X = 0] = \Pr[B = 1 \mid X = 1] = b$$

and $P_{Y|B=0,X=0} = P_{Y|B=0,X=1}$. We have

$$\Pr[X = x \mid B = 0] = \frac{\Pr[X = x] \cdot (1 - b)}{\Pr[X = 0] \cdot (1 - b) + \Pr[X = 1] \cdot (1 - b)} = \Pr[X = x] \ .$$

From Lemma 5 follows that

$$\begin{aligned} \mathrm{PredAdv}(X \mid Y) &\leq (1 - b) \cdot \mathrm{PredAdv}(X \mid Y, B = 0) + b \cdot \mathrm{PredAdv}(X \mid Y, B = 1) \\ &\leq (1 - b) \cdot \mathrm{PredAdv}(X \mid B = 0) + b \\ &\leq (1 - b) \cdot a + b \\ &= 1 - (1 - a)(1 - b) \ . \end{aligned}$$

Note that $\mathrm{PredAdv}(X \mid B = 0) = \mathrm{PredAdv}(X)$. □

A.2 Proofs of Section 3

Proof of Theorem 2. We choose $g := (1-2\varepsilon)(1-d)+qd$ and use Protocol $\mathsf{SimWEC}(d, \varepsilon, g)$. We get

$$\Pr[Y = \Delta] = g\left(1 - \frac{(1 - 2\varepsilon)(1 - d)}{g}\right) + (1 - g)\left(1 - \frac{2\varepsilon(1 - d)}{1 - g}\right) = d$$

and

$$\Pr[X \neq Y \mid Y \neq \Delta] = \frac{\frac{1}{2} \cdot 2\varepsilon(1 - d)}{2\varepsilon(1 - d) + (1 - 2\varepsilon)(1 - d)} = \varepsilon \ .$$

Therefore

$$\Pr[M = X \mid Y = \Delta] = \frac{\Pr[M = X, Y = \Delta]}{\Pr[Y = \Delta]} = \frac{g - (1 - 2\varepsilon)(1 - d)}{d} \tag{A.1}$$

and hence

$$\begin{aligned} \mathrm{PredAdv}(X \mid M, Y = \Delta) &= \Pr[M = X \mid Y = \Delta] \\ &= \frac{g - (1 - 2\varepsilon)(1 - d)}{d} = q \ . \end{aligned}$$

Furthermore, we have

$$\Pr[M = X \mid Y \neq \Delta] = \frac{\Pr[M = X, Y \neq \Delta]}{\Pr[Y \neq \Delta]} = \frac{(1 - 2\varepsilon)(1 - d)}{1 - d} = 1 - 2\varepsilon \ .$$

Using Eq. A.1, we get

$$\begin{aligned} \delta(P_{XU|Y\neq\Delta}, P_{XU|Y=\Delta}) &= \left|\Pr[M = X \mid Y \neq \Delta] - \Pr[M = X \mid Y = \Delta]\right| \\ &= \left|1 - 2\varepsilon - \frac{g - (1 - 2\varepsilon)(1 - d)}{d}\right| \\ &= \frac{1 - g - 2\varepsilon}{d} \\ &= 1 - 2\varepsilon - q \leq p \ . \end{aligned}$$

□

Proof of Theorem 3. In the following, let $X = (X_0, X_1)$ be the output of the honest sender, C and Y be the outputs of the honest receiver, and $E = Y \oplus X_C$.

From Lemma 20 follows that in every iteration, the probability of the protocol to terminate is at least $\min(2d_0(1-d_0), 2d_1(1-d_1))$, from which follows that the expected number of instances used by this protocol is at most $1/\min(2d_0(1-d_0), 2d_1(1-d_1))$. If the protocol terminates, the output is equal to the value that is not Δ. By the definition of $\mathsf{PassiveWEC}$, the output is correct with a probability of at least $1 - \varepsilon$.

Let V be the additional output of the dishonest receiver. We have $V = (C, Y, Y_0, Y_1, V_0, V_1)$, where Y_0 and Y_1 are the the outputs of the honest, and V_0 and V_1 the additional outputs of the dishonest receiver of the two instances of $\mathsf{PassiveWEC}$ in the last round. All the outputs of the other rounds are independent and can be omitted. Since two instances of $\mathsf{PassiveWEC}$ in the last round are independent of each other, we get

$$\begin{aligned}\mathrm{PredAdv}(X_{1-C} \mid V, E) &= \mathrm{PredAdv}(X_{1-C} \mid C, Y, Y_0, Y_1, V_0, V_1, E, Y_C \neq \Delta, Y_{1-C} = \Delta)\\ &= \mathrm{PredAdv}(X_{1-C} \mid V_{1-C}, Y_{1-C} = \Delta) \leq q\ .\end{aligned}$$

Let U be the additional output of the dishonest sender. We have $U = (X, U_0, U_1)$, where U_0 and U_1 are the additional outputs of the dishonest sender of the two instances of $\mathsf{PassiveWEC}$ in the last round. Again, all the outputs of the other rounds are independent and can be omitted. We can apply Lemma 3 for U_0 and U_1, which gives us two independent random variables B_0 and B_1, such that for $i \in \{0,1\}$ and $x_i \in \{0,1\}$,

$$P_{X_i U_i | Y_i \neq \Delta, B_i = 0} = P_{X_i U_i | Y_i = \Delta, B_i = 0}$$

and

$$\Pr[B_i = 1 \mid Y_i \neq \Delta] = \Pr[B_i = 1 \mid Y_i = \Delta] = p\ .$$

Let $B = \max(B_0, B_1)$. Note that for $(Y_0 = \Delta, Y_1 \neq \Delta)$ we have $C = 1$ and for $(Y_0 \neq \Delta, Y_1 = \Delta)$ we have $C = 0$, and that one of the two cases must occur. We get

$$\Pr[B = 1 \mid C = 0] = \Pr[B = 1 \mid C = 1] = 1 - (1-p)^2$$

and

$$P_{X_0 U_0 X_1 U_1 | C=0, B=0} = P_{X_0 U_0 X_1 U_1 | C=1, B=0}\ .$$

From Lemma 1 follows that

$$\delta(P_{X_0 U_0 X_1 U_1 | C=0}, P_{X_0 U_0 X_1 U_1 | C=1}) \leq 1 - (1-p)^2\ .$$

From Lemma 19 follows that C is maximally biased if $\Pr[Y_0 = \Delta] = d_0$ and $\Pr[Y_1 = \Delta] = d_1$ (or vice versa). It follows that

$$\mathrm{PredAdv}(C) \leq 2\frac{d_1(1-d_0)}{d_1(1-d_0) + d_0(1-d_1)} - 1 = 1 - 2\frac{d_0(1-d_1)}{d_1(1-d_0) + d_0(1-d_1)}\ .$$

Finally, it follows from Lemma 6 that

$$\mathrm{PredAdv}(C \mid U) = \mathrm{PredAdv}(C \mid U_0, U_1, X) \leq 1 - 2\frac{d_0(1-d_1)}{d_1(1-d_0) + d_0(1-d_1)}(1-p)^2\ .$$

□

Note that for the stronger requirement of $\mathrm{PredAdv}(C \mid U, E)$ from the definition of WOT in [Wul07], we would not be able to achieve the same bound: If, for example, the first $\mathsf{PassiveWEC}$ always has an error with probability ε, but the the second has no error, then knowing that an error occurred would tell the sender that $C = 0$.

A.3 Proofs of Section 4

Proof of Theorem 4. We have $\Pr[Y \neq X] = \varepsilon_A(1-\varepsilon_B)+(1-\varepsilon_A)\varepsilon_B = \varepsilon$, and $\Pr[Y = X] = 1-\varepsilon$. We have $U = M$ and $V = M$, where M is the transmitted message. We have

$$\begin{aligned}\delta(P_{UX|Y=X}, P_{UX|Y\neq X}) &= 2\Pr[M = X = 0 \mid Y = X] - 2\Pr[M = X = 0 \mid Y \neq X] \\ &= \frac{(1-\varepsilon_A)(1-\varepsilon_B)}{1-\varepsilon} - \frac{\varepsilon_A(1-\varepsilon_B)}{\varepsilon} \;.\end{aligned}$$

and for all $y \in \{0,1\}$

$$\begin{aligned}\delta(P_{V|X=0,Y=y}, P_{V|X=1,Y=y}) &= \Pr[M = 0 \mid X = 0, Y = y] - \Pr[M = 0 \mid X = 1, Y = y] \\ &= \frac{(1-\varepsilon_A)(1-\varepsilon_B)}{1-\varepsilon} - \frac{(1-\varepsilon_A)\varepsilon_B}{\varepsilon} \;.\end{aligned}$$

□

Proof of Theorem 5. Let $c := \Pr[Y_0 \neq X_0]$ and $c' := \Pr[Y_1 \neq X_1]$. We get

$$\Pr[Y \neq X \mid Y \neq \Delta] = \frac{cc'}{cc' + (1-c)(1-c')} \;.$$

Since $c, c' \in [\varepsilon_0, \varepsilon_1]$ it follows from Lemma 18 that

$$\Pr[Y \neq X \mid Y \neq \Delta] \leq \frac{\varepsilon_1^2}{\varepsilon_1^2 + (1-\varepsilon_1)^2} \;.$$

Furthermore, from Lemma 20 follows that

$$\Pr[Y = \Delta] = c(1-c') + c'(1-c) \in [d_0, d_1] \;.$$

Let V_0 and V_1 be the additional information a dishonest receiver gets in the two executions of the PassiveWBSC. We have $V := (K, V_0, V_1, Y_0, Y_1)$. Using Lemma 3, we can define two random variables B_0 and B_1 such that

$$\Pr[B_0 = 1 \mid X_0 = 0, Y_0 = y_0] = \Pr[B_0 = 1 \mid X_0 = 1, Y_0 = y_0] \;,$$

$$\Pr[B_1 = 1 \mid X_1 = 0, Y_1 = y_1] = \Pr[B_1 = 1 \mid X_1 = 1, Y_1 = y_1] = q \;,$$

$$P_{V_0|X_0=0,Y_0=y_0,B_0=0} = P_{V_0|X_0=1,Y_0=y_0,B_0=0}$$

and

$$P_{V_1|X_1=0,Y_1=y_1,B_1=0} = P_{V_1|X_1=1,Y_1=y_1,B_1=0} \;.$$

Note that (V_0, X_0, Y_0, B_0) and (V_0, X_1, Y_1, B_1) are independent, $x_0 \oplus x_1 = k$, and $Y = \Delta$ if and only if $y_1 = y_0 \oplus k \oplus 1$. Let $B := \max(B_0, B_1)$. We get

$$P_{V_0V_1|X=0,K=k,Y_0=y_0,Y_1=y_1,Y=\Delta,B=0} = P_{V_0V_1|X=1,K=k,Y_0=y_0,Y_1=y_1,Y=\Delta,B=0} \qquad \text{(A.2)}$$

and

$$\Pr[B = 1 \mid X = x, K = k, Y_0 = y_0, Y_1 = y_1, Y = \Delta] = \frac{(1-p)^2 \cdot 2 \cdot \frac{1}{2}\varepsilon_0 \cdot \frac{1}{2}(1-\varepsilon_0)}{2 \cdot \frac{1}{2}\varepsilon_0 \cdot \frac{1}{2}(1-\varepsilon_0)} = (1-q)^2 \;.$$

It follows from Lemma 1 that

$$\delta(P_{V_0V_1|X=0,K=k,Y_0=y_0,Y_1=y_1}, P_{V_0V_1|X=1,K=k,Y_0=y_0,Y_1=y_1}) \leq 1 - (1-q)^2 \;.$$

We can bound

$$\begin{aligned}
&\Pr[X = x \mid Y_0 = y_0, Y_1 = y_1, K = k, Y = \Delta] \\
&\quad \le \frac{\frac{1+\varepsilon}{2}\varepsilon_1 \cdot \frac{1+\varepsilon}{2}(1-\varepsilon_0)}{\frac{1+\varepsilon}{2}\varepsilon_1 \cdot \frac{1+\varepsilon}{2}(1-\varepsilon_0) + \frac{1-\varepsilon}{2}\varepsilon_0 \cdot \frac{1-\varepsilon}{2}(1-\varepsilon_1)} , \\
&\quad = \frac{(1+\varepsilon)\varepsilon_1 \cdot (1+\varepsilon)(1-\varepsilon_0)}{(1+\varepsilon)\varepsilon_1 \cdot (1+\varepsilon)(1-\varepsilon_0) + (1-\varepsilon)\varepsilon_0 \cdot (1-\varepsilon)(1-\varepsilon_1)} ,
\end{aligned}$$

from which follows

$$\begin{aligned}
&\mathrm{PredAdv}(X \mid Y_0 = y_0, Y_1 = y_1, K = k, Y = \Delta) \\
&\quad = 2 \max_x \Pr[X = x \mid Y_0 = y_0, Y_1 = y_1, K = k, Y = \Delta] - 1 \\
&\quad \le \frac{\varepsilon_1 - \varepsilon_0}{\varepsilon_1 + \varepsilon_0 - 2\varepsilon_0\varepsilon_1} + \frac{2\varepsilon}{1+\varepsilon^2} .
\end{aligned}$$

Using Lemma 6, we get

$$\mathrm{PredAdv}(X \mid V, Y = \Delta) = 1 - \left(1 - \frac{\varepsilon_1 - \varepsilon_0}{\varepsilon_1 + \varepsilon_0 - 2\varepsilon_0\varepsilon_1} - \frac{2\varepsilon}{1+\varepsilon^2}\right)(1-q)^2 .$$

Let U_0 and U_1 be the additional information a dishonest sender gets in the two executions of the PassiveWBSC. We have $U = (X_0, X_1, U_0, U_1)$. For $j \in \{0,1\}$, we have

$$\delta(P_{X_j U_j | Y_j = X_j}, P_{X_j U_j | Y_j \neq X_j}) \le p .$$

Let B_j be random variables as defined by Lemma 3. So

$$\Pr[B_j = 1 \mid Y_j = X_j] = \Pr[B_j = 1 \mid Y_j \neq X_j] = p$$

and

$$P_{X_j U_j | Y_j = X_j, B_j = 0} = P_{X_j U_j | Y_j \neq X_j, B_j = 0} .$$

Let $B := \max(B_0, B_1)$. We get

$$\Pr[B = 1 \mid Y = \Delta] = \Pr[B = 1 \mid Y \neq \Delta] = 1 - (1-p)^2$$

and

$$\delta(P_{XU|Y=\Delta, B=0}, P_{XU|Y\neq\Delta, B=0}) = 0 .$$

Hence, it follow from Lemma 1 that

$$\delta(P_{XU|Y=\Delta}, P_{XU|Y\neq\Delta}) \le 1 - (1-p)^2 .$$

□

A.3.1 PassiveWBSC from PassiveUNC

Definition 7. Let $0 \le \gamma \le \delta < \frac{1}{2}$. A (δ,γ)-PassiveUNC is a primitive that takes as input $x \in \{0,1\}$ from the sender and outputs $y \in \{0,1\}$ to the receiver, where $y \neq x$ with probability δ. Let $\mu := \frac{\delta-\gamma}{1-2\gamma}$. If the sender is cheating, then the channel first calculates u such that $u \neq x$ has a probability γ, and then y such that $y \neq u$ has a probability of μ, and sends u to the sender and y to the receiver. If the receiver is cheating, then the channel first calculates v such that $v \neq x$ has a probability μ, and then y such that $y \neq u$ has a probability of γ, and sends (y,v) to the receiver.

Note that no matter who cheats, $y \neq x$ has always the same probability δ.

Lemma 7. *Let*

$$p := \frac{(1-\delta)\delta - (1-\gamma)\gamma}{(1-2\gamma)\delta(1-\delta)} \ .$$

If the sender chooses her input uniformly, then (δ, γ)-PassiveUNC is a $(0, \delta, \delta, p, p)$-PassiveWBSC.

Proof.

$$\begin{aligned}\delta(P_{UX|Y=X}, P_{UX|Y\neq X}) &= \Pr[U = X \mid Y = X] - \Pr[U = X \mid Y \neq X] \\ &= 2\Pr[U = X = 0 \mid Y = X] - 2\Pr[U = X = 0 \mid Y \neq X] \\ &= \frac{(1-\gamma)(1-\mu)}{1-\delta} - \frac{\gamma(1-\mu)}{\delta} = p \ .\end{aligned}$$

Furthermore, for all $y \in \{0, 1\}$

$$\begin{aligned}\delta(P_{V|X=0,Y=y}, P_{V|X=1,Y=y}) &= \Pr[V = y \mid X = y, Y = y] - \Pr[V = y \mid X \neq y, Y = y] \\ &= \frac{(1-\mu)(1-\gamma)}{1-\delta} - \frac{(1-\mu)\gamma}{\delta} = p \ .\end{aligned}$$

□

A.4 Proofs from Section 5

Proof of Theorem 6. First of all, using coin-toss, it is easy to make Protocol SimWEC work in the malicious model. The proof is very similar to the proof of Theorem 4. We have

$$\begin{aligned}\delta(P_{U|Y\neq\Delta}, P_{U|Y=\Delta}) &\leq \big|\Pr[M = X \mid T \neq \Delta] - \Pr[M = X \mid T \neq \Delta]\big| \\ &= \frac{1-g-2\varepsilon}{d} \leq p \ .\end{aligned}$$

g is the probability with which the receiver gets X, and hence we have $\mathrm{PredAdv}(X \mid M) \leq g$. □

A.4.1 Bit Commitment from ActiveWEC

Let us start with some definitions and lemmas. The *conditional smooth min-entropy of X given Y* [RW05] is defined as

$$H^{\varepsilon}_{\min}(X \mid Y) := \min_{\Omega:\Pr[\Omega]\geq 1-\varepsilon} \min_{xy}(-\log P_{X\Omega|Y=y}(x)) \ .$$

Lemma 8 ([Cac97, MW97, RW05])**.** $H^{\varepsilon+\varepsilon'}_{\min}(X \mid YZ) \geq H^{\varepsilon}_{\min}(XY \mid Z) - \log|\mathcal{Y}| - \log(1/\varepsilon')$.

Lemma 9 (Leftover hash lemma [BBR88, ILL89])**.** *Let X be a random variable over $\mathcal{X}$ and let $m > 0$. Let $h : \mathcal{S} \times \mathcal{X} \rightarrow \{0,1\}^m$ be a 2-universal hash function. If $m \leq H^{\varepsilon}_{\min}(X \mid Y) - 2\log(1/\varepsilon')$, then for S uniform over $\mathcal{S}$, $h(S, X)$ is $(\varepsilon + \varepsilon')$-close to uniform with respect to (S, Y).*

Note that for our choices of κ, c and n, we have $\kappa \geq \exp(-2(1 - d_1 - c)nc^2) \geq \exp(-2nc^2)$.

Lemma 10. *If both players are honest, then Protocol ActiveWECtoBC aborts with a probability at most 3κ.*

Proof. From Lemma 17 follows that the number of $y_i = \Delta$ is outside the interval $[(d_0 - c) \cdot n - 1, (d_1 + c) \cdot n]$ with probability at most $2\exp\left(-2nc^2\right) \leq 2\kappa$. Given that this is not the case, the probability that the number of values y_i that is not equal to Δ nor x_i is bigger than $(\varepsilon + c) \cdot (n - n_\Delta)$ is at most $\exp\left(-2(n - n_\Delta)c^2\right) \leq \exp\left(-2(1 - d_1 - c)nc^2\right) \leq \kappa$. □

Lemma 11. *Protocol ActiveWECtoBC is binding with probability* $1 - 4\kappa$.

Proof. According to Lemma 3, for all i there exist random variables B_i, such that

$$\Pr[B_i = 1 \mid Y_i = \Delta] = \Pr[B_i = 1 \mid Y_i \neq \Delta] = p ,$$

and

$$P_{U_i|Y_i=\Delta,B_i=0} = P_{U_i|Y_i\neq\Delta,B_i=0} .$$

Let the random variable $Y_i' \in \{0,1\}$ be defined as follows: If $Y_i \neq \Delta$, let $Y_i' = Y_i$, and let Y_i' be chosen randomly from $\{0,1\}$ otherwise, such that $\Pr[Y_i' = 1 \mid Y_i = \Delta] = \Pr[Y_i' = 1 \mid Y_i \neq \Delta]$. ($Y_i'$ is therefore equal to Y_i, but without the erasures, and is independent of the event $Y_i = \Delta$.) Let us assume that the sender additionally receives the values B_i and Y_i'.

We divide the n instances into 3 sets. The first set is the set S_0 of values where $B_i = 1 \wedge Y_i = \Delta$, the second set S_1 is the set of values where $B_i = 1 \wedge Y_i \neq \Delta$, and the third set S_2 is the set of values where $B_i = 0$. Let $d := n_\Delta/n$. The receiver will only accept if $d \in [d_0 - c, d_1 + c]$. Since $\kappa \geq \exp(-2nc^2)$, it follows from Lemma 17 that with probability $1 - 3\kappa$, $|S_0| \leq (dp + c)n$, $|S_1| \leq ((1-d)p + c)n$ and $|S_2| \leq (1 - p + c)n$. The sender can freely choose all the values x_i in set S_0, as she knows that the receiver cannot check them. Since the receiver allows a certain amount of errors, the sender may choose a subset of S_1 of size a and a subset of S_2 of size b, where $x_i \neq y_i'$. We know that the receiver will notice all a errors in S_1, and it follows from Lemma 17 that with probability $1 - \kappa$, he will notice at least

$$b \cdot \left(1 - d - \sqrt{\frac{1}{2b} \cdot \ln\frac{1}{\kappa}}\right) = b \cdot (1-d) - \sqrt{\frac{b}{2} \cdot \ln\frac{1}{\kappa}}$$

from S_2. Therefore, the receiver will only accept with probability at least κ, if

$$a + b \cdot (1-d) - \sqrt{\frac{b}{2} \cdot \ln\frac{1}{\kappa}} \leq (\varepsilon + c)(1-d)n .$$

The sender would only be able to find two values with the same parity-check, if

$$(dp + c)n + 2(a + b) \geq m .$$

The best strategy for the sender is to choose $a = 0$, and to make b maximal. It follows from the definition of m that the sender cannot find two such values. The statement follows. □

Lemma 12. *Protocol ActiveWECtoBC is hiding with probability* $1 - 3\kappa$.

Proof. The sender holds $X = (X_1, \ldots, X_n)$, and the receiver $V = (V_1, \ldots V_n)$, S and the auxiliary input z. Using Lemma 3, for every pair (X_i, V_i), there exists a random variable B_i, such that $\Pr[B_i = 1] = g$ and $P_{V_i|X=0,B_i=0,Z=z} = P_{V_i|X=1,B_i=0,Z=z}$. From Lemma 17 follows that with probability $1 - \kappa$, the number of $B_i = 0$ is at least $n(1 - g - c)$. Since X_i is uniform given V_i and $B_i = 0$, we have

$$H_\infty^\kappa(X \mid V, Z = z) \geq n(1 - g - c) .$$

Using Lemma 8, we get

$$H_\infty^{2\kappa}(X \mid V, S, Z = z) \geq n(1 - g - c) - (n - k) - \log(1/\kappa) .$$

Finally, we can apply Lemma 9, and get that $g(X, R)$ is 3κ-close to uniform, since

$$\ell \leq H_\infty^{2\kappa}(X \mid V, S, Z = z) - 2\log(1/\kappa) \ .$$

□

The statement of Theorem 7 follows from Lemma 10, 11 and 12.

A.4.2 PassiveWEC from ActiveWEC

Proof of Lemma 4. Let B be the random variable defined by Lemma 2. We have

$$\Pr[B = 1] = g \ ,$$

and

$$P_{V|X=0,B=0} = P_{V|X=1,B=0} \ .$$

Given $B = 0$, V does not have any information about X. Hence, for any $Y = f(V)$, we have

$$\Pr[Y \neq X \mid Y \neq \Delta] \geq \frac{1}{2} \cdot \frac{\Pr[Y \neq \Delta \wedge B = 0]}{\Pr[Y \neq \Delta]} \ .$$

Therefore, it must hold that

$$2\varepsilon \Pr[Y \neq \Delta] \geq \Pr[Y \neq \Delta \wedge B = 0] \ .$$

From

$$\Pr[Y \neq \Delta \wedge B = 1] = \Pr[Y \neq \Delta] - \Pr[Y \neq \Delta \wedge B = 0]$$

and

$$\Pr[Y = \Delta \wedge B = 1] = g - \Pr[Y \neq \Delta \wedge B = 1]$$

we get

$$\Pr[Y = \Delta \wedge B = 1] = g - \Pr[Y \neq \Delta] + \Pr[Y \neq \Delta \wedge B = 0] \ .$$

Therefore

$$\begin{aligned}\Pr[B = 1 \mid Y = \Delta] &= \frac{g - \Pr[Y \neq \Delta] + \Pr[Y \neq \Delta \wedge B = 0]}{\Pr[Y = \Delta]} \leq \frac{g - \Pr[Y \neq \Delta] + 2\varepsilon \Pr[Y \neq \Delta]}{\Pr[Y = \Delta]} \\ &\leq \frac{g - (1 - 2\varepsilon)(1 - \Pr[Y = \Delta])}{\Pr[Y = \Delta]} = 1 - 2\varepsilon - \frac{1 - g - 2\varepsilon}{\Pr[Y = \Delta]} \\ &\leq 1 - 2\varepsilon - \frac{1 - g - 2\varepsilon}{d_1} = \frac{g - (1 - 2\varepsilon)(1 - d_1)}{d_1} \ .\end{aligned}$$

The statement follows now by applying Lemma 1. □

Lemma 13. *If both players are honest, then Protocol ActiveToPassiveWEC aborts with a probability smaller than 3κ.*

Proof. From Lemma 17 follows that the number of $y_i = \Delta$ is outside the interval $[(d_0 - c) \cdot n - 1, (d_1 + c) \cdot n]$ with probability at most $2\exp\left(-2nc^2\right) \leq 2\kappa$. Given that this is not the case, the probability that the number of values y_i that is not equal to Δ nor x_i is bigger than $(\varepsilon + c) \cdot (n - n_\Delta)$ is at most $\exp\left(-2(n - n_\Delta)c^2\right) \leq \exp\left(-2(1 - d_1 - c)nc^2\right) \leq \kappa$. If these two conditions hold, then the players will not abort, checking all but one values. □

Lemma 14. *If neither of the players aborts the protocol, then both are committed to values X and Y, where $\Pr[Y = \Delta] \in [d_0 - 2c, d_1 + 2c]$ and $\Pr[Y \neq X \mid Y \neq \Delta] \leq \varepsilon + 2c$.*

Proof. The number of values $y_i = \Delta$ is either n_Δ or $n_\Delta + 1$. Since S is chosen at random, we have

$$\Pr[Y = \Delta] \in \left[\frac{n_\Delta}{n}, \frac{n_\Delta + 1}{n}\right] \subseteq \left[d_0 - c - \frac{1}{n}, d_1 + c + \frac{1}{n}\right] \subseteq [d_0 - 2c, d_1 + 2c] \ ,$$

holds and

$$\Pr[Y \neq X \mid Y \neq \Delta] \leq \frac{(\varepsilon + c)(n - n_\Delta) + 1}{n - n_\Delta} = \varepsilon + c + \frac{1}{n - n_\Delta} \leq \varepsilon + 2c \ .$$

□

Lemma 15. *If the receiver is honest, then for any malicious sender, the execution of Protocol* ActiveToPassiveWEC *is either aborted or the sender and the receiver are committed to values X and Y, where $\delta(P_{XU|Y\neq\Delta}, P_{XU|Y=\Delta}) \leq p$.*

Proof. The adversary calculates X from U. It follows directly that

$$\delta(P_{XU|Y\neq\Delta}, P_{XU|Y=\Delta}) \leq p \ .$$

□

Lemma 16. *If the sender is honest, then for any malicious receiver, the execution of Protocol* ActiveToPassiveWEC *is either aborted or the sender and the receiver are committed to values X and Y where*

$$\delta(P_{V|X=0,Y=\Delta}, P_{V|X=1,Y=\Delta}) \leq \frac{g - (1 - 2\varepsilon)(1 - d_1)}{d_1} + \frac{4}{d_1^2} c \ .$$

Proof. The adversary calculates Y using his additional information V. We can apply Lemmas 4, 14 and 21 and we get

$$\begin{aligned}
\delta(P_{V|X=0,Y=\Delta}, P_{V|X=1,Y=\Delta}) &\leq \frac{g - (1 - 2\varepsilon - 2c)(1 - d_1 - 2c)}{d_1 + 2c} \\
&= 1 - 2\varepsilon - 2c - \frac{1 - g - 2\varepsilon}{d_1 + 2c} + \frac{2}{d_1 + 2c} c \\
&\leq 1 - 2\varepsilon - \frac{1 - g - 2\varepsilon}{d_1} + 2\frac{1 - g - 2\varepsilon}{d_1^2} c + \frac{2}{d_1 + 2c} c \\
&= \frac{g - (1 - 2\varepsilon)(1 - d_1)}{d_1} + \left(2\frac{1 - g - 2\varepsilon}{d_1^2} + \frac{2}{d_1 + 2c}\right) c \\
&\leq \frac{g - (1 - 2\varepsilon)(1 - d_1)}{d_1} + \frac{4}{d_1^2} c
\end{aligned}$$

□

The statement of Theorem 8 follows from Lemmas 13, 15 and 16.

A.5 Technicalities

Lemma 17 (Chernoff/Hoeffding bound)**.** *Let $P_{X_0 \dots X_n} = P_{X_0} \dots P_{X_n}$ be a product distribution with $X_i \in [0,1]$. Let $\overline{X} := \frac{1}{n}\sum_{i=0}^{n-1} X_i$, and $\mu = E[\overline{X}]$. Then, for any $\varepsilon > 0$,*

$$\Pr\left[\overline{X} \geq \mu + \varepsilon\right] \leq \exp\left(-2n\varepsilon^2\right) \ , \qquad \Pr\left[\overline{X} \leq \mu - \varepsilon\right] \leq \exp\left(-2n\varepsilon^2\right) \ .$$

Lemma 18. *Let $0 \leq e_0 \leq e_1 \leq 1$. Then*

$$\max_{c,c' \in [e_0,e_1]} \frac{cc'}{cc' + (1-c)(1-c')} \leq \frac{e_1^2}{e_1^2 + (1-e_1)(1-e_1)} \ .$$

Proof. Let $f(x,y) := \frac{xy}{xy+(1-x)(1-y)}$. We have

$$\frac{\partial}{\partial x} f(x,y) = \frac{y(1-y)}{(xy + (1-x)(1-y))^2} \geq 0 \ , \qquad \frac{\partial}{\partial y} f(x,y) = \frac{x(1-x)}{(xy + (1-x)(1-y))^2} \geq 0 \ .$$

Hence, $f(x,y)$ is maximized on $x, y \in [e_0, e_1]$ for $x = y = e_1$. □

Lemma 19. *Let $0 \leq d_0 \leq d_1 \leq 1$. Then*

$$\max_{d,d' \in [d_0,d_1]} \frac{d(1-d')}{d(1-d') + d'(1-d)} \leq \frac{d_1(1-d_0)}{d_1(1-d_0) + d_0(1-d_1)} \ .$$

Proof. Let $f(x,y) := \frac{x(1-y)}{x(1-y)+x(1-y)}$. We have

$$\frac{\partial}{\partial x} f(x,y) = \frac{y(1-y)}{(x(1-y) + x(1-y))^2} \geq 0 \ , \qquad \frac{\partial}{\partial y} f(x,y) = \frac{-x(1-x)}{(x(1-y) + x(1-y))^2} \leq 0 \ .$$

Hence, $f(x,y)$ is maximized on $x, y \in [d_0, d_1]$ for $x = d_1$ and $y = d_0$. □

Lemma 20. *Let $0 \leq d_0 \leq d_1 \leq 1$. Then*

$$\min_{x,y \in [d_0,d_1]} x(1-y) + y(1-x) = \min(2d_0(1-d_0), 2d_1(1-d_1))$$

and

$$\max_{x,y \in [d_0,d_1]} x(1-y) + y(1-x) = \max(2d_0(1-d_0), 2d_1(1-d_1), d_1(1-d_0) + d_0(1-d_1)) \ .$$

Proof. Let $f(x,y) := x(1-y) + y(1-x)$ We have

$$\frac{\partial}{\partial x} f(x,y) = 1 - 2y \ , \qquad \frac{\partial}{\partial y} f(x,y) = 1 - 2x \ .$$

Since these functions are linear, $f(x,y)$ can only be minimized or maximized on one of the four corner points, where both x and y are either equal to d_0 or d_1. Furthermore, if $d_0 \leq 0.5$ then $f(d_0,d_0) \leq f(d_0,d_1)$ and $f(d_0,d_0) \leq f(d_1,d_0)$. Similarly, if $d_1 \geq 0.5$, then $f(d_1,d_1) \leq f(d_0,d_1)$ and $f(d_1,d_1) \leq f(d_1,d_0)$. Therefore, the function can only be at its minimal when $x = y$. □

Lemma 21. *For $a, b, c > 0$, we have*

$$\frac{a}{b+c} \geq \frac{a}{b} - \frac{a}{b^2} c \ .$$

Proof.

$$\frac{a}{b+c} = \frac{ab}{b(b+c)} = \frac{a(b+c) - ac}{b(b+c)} = \frac{a}{b} - \frac{ac}{b^2 + bc} \geq \frac{a}{b} - \frac{ac}{b^2}$$

□