Bit Commitment from Non-Local Correlations

Severin Winkler, Stefan Wolf and Jürg Wullschleger

Abstract—Central cryptographic functionalities such as encryption, authentication, or secure two-party computation cannot be realized in an information-theoretically secure way from scratch. This serves as a motivation to study what (possibly weak) primitives they can be based on. We consider as such starting points general two-party input-output systems that do not allow for message transmission, and show that they can be used for realizing unconditionally secure bit commitment as soon as they are non-trivial, i.e., cannot be realized from distributed randomness only. In particular, our result implies that any two-qubit state without hidden-variable model has an input-output behavior allowing for unconditional bit commitment.

Index Terms—Unconditional security, bit commitment, non-locality.

I. INTRODUCTION

A. Bit Commitment

Modern cryptography deals — besides the classical tasks of encryption and authentication — with secure cooperation between two (or more) parties willing to collaborate but mistrusting each other. Examples of important functionalities of such secure two-party computation are bit commitment and oblivious transfer. In this note, we concentrate on bit commitment, a primitive which, for instance, allows for fair coin flipping over the telephone [Blu83] and has central applications in interactive proof systems.

A bit commitment scheme is a pair of protocols, commit and open, executed by two parties, Alice and Bob. First, they execute commit where Alice chooses a bit $b$ as input. Later, they execute open where Alice reveals the bit $b$ to Bob. The security properties of bit commitment are the following. Security for Alice ensures that the commitment is hiding: The commit protocol should not give any information about the bit $b$ to Bob. Security for Bob, on the other hand, means that after the execution of commit, $b$ cannot be changed anymore by Alice. Ideally, one would like these security properties to hold in an information-theoretically secure way.

It is well known that bit commitment that is unconditionally secure for both parties cannot be implemented from (noiseless) classical communnication only — and the same is true even for (noiseless) quantum communication [May97], [LC97]. If one is not willing to reduce the security to being computational for one party or the other, it becomes a natural question what information-theoretic primitives allow for realizing unconditionally secure bit commitment. This question has been studied intensively by many authors already, and several optimistic results have been obtained: Bit commitment can be realized from communication over noisy channels [Cre97], [WNI03] or from pieces of correlated randomness [IMQNW04], [WW04], [IMNW06]. The present article corrects and strongly extends preliminary results presented in [WW05a].

B. Non-Local Correlations

Motivated by the fact that entangled quantum states can show a so-called non-local behavior, the question has been studied whether such correlations allow for realizing cryptographic primitives in an unconditionally secure way as well. A two-party input-output system is characterized by a conditional distribution $P_{XY|UV}$, where $U$ and $V$ stand for the inputs and $X$ and $Y$ for the outputs to the systems on the left and right hand sides of the system, respectively. Intuitively speaking, such a system is non-local if its behavior cannot be explained by pre-determined information. On the other hand, we only consider correlations that are, at the same time, non-signaling, i.e., which do not allow for message transmission from one side to the other. An example of such a system is the non-local box (NL box for short) proposed by Popescu and Rohrlich [PR97], the behavior of which is as follows: All variables are binary, each output is a uniform bit, independent of the pair of inputs, but $X \oplus Y = U \land V$ always holds. Interestingly, an NL box is, cryptographically speaking, the same as one-out-of-two bit oblivious transfer [WW05b] and, hence, does allow for realizing bit commitment as well. It has been argued that this did not contradict Mayers’ no-go result because the classical system does, in contrast to a shared quantum state, not allow for a delay of one of the inputs, i.e., provides no output on either side before both inputs are given (a property that, actually, makes it signaling) [SGP05]. However, this explanation turned out to be wrong: NL boxes with delay still allow for bit commitment [BCU+06]. A second explanation that was given is that NL boxes are more non-local than any quantum state. In contradiction to this intuition, we show that any non-local system providing binary outputs allows for unconditionally secure bit commitment. More precisely, we show an all-or-nothing result on such systems (Theorem 3): They are either simulatable with shared randomness, or allow for unconditional bit commitment; our condition is thus tight. This also means that the crucial difference to Mayers’ result is that there, entangling attacks are possible, whereas we only consider the states’ classical behavior.
II. Preliminaries

A. Bit Commitment

A bit commitment scheme is a pair of protocols Commit and Open executed by two parties Alice and Bob. First, Alice and Bob execute Commit where Alice has a bit as input. Bob either accepts or rejects the execution of Commit. Later, they execute Open where Bob has output (accept, b) or reject. The two protocols must have the following (ideal) properties:

- Correctness: If both parties follow the protocol, then Bob always accepts with b' = b.
- Hiding: If Alice is honest, then committing to b does not reveal any information about b to Bob[1].
- Binding: If Bob is honest and accepts after the execution of Commit, then there exists only one value b' (which is equal to b, if Alice is honest) that Bob accepts as output after the execution of Open.

In the following we call a bit commitment scheme secure, if it fulfills the above ideal requirements except with an error that can be made negligible (as a function of some security parameter n).

B. Notation

Let \( W : \mathcal{X} \rightarrow \mathcal{Y} \) be a stochastic matrix with rows indexed by elements of \( \mathcal{X} \) and columns indexed by elements of \( \mathcal{Y} \). We denote the entries of \( W \) by \( W(y|x) = W_{xy} \) and the row vector indexed by \( x \) by \( W_x \). \( W_x(\cdot) \) defines a probability distribution on \( \mathcal{Y} \) for every \( x \in \mathcal{X} \), i.e., for all \( x \) it holds that

\[
W(y|x) \geq 0 \quad \forall y,
\]

\[
\sum_y W(y|x) = 1.
\]

We denote by \( \text{conv}(W) \) the convex hull of the set \( \{W_x|x \in \mathcal{X}\} \), i.e., the convex hull of the row vectors of \( W \). We call \( W_x \) an extreme point of this set if the convex hull of the set \( \{(W_x|x \in \mathcal{X})\} \) is strictly smaller. We denote the set of extreme points by \( \text{extr}(\text{conv}(W)) \). We call \( W_x \) non-extreme if it is not an extreme point of \( \text{conv}(W) \). We denote by \( x^n = (x_1, \ldots, x_n) \) a sequence of elements in \( \mathcal{X} \) or a vector in \( \mathcal{X}^n \). If \( I := \{i_1, \ldots, i_k\} \subseteq \{1, 2, \ldots, n\} \) then \( x^I \) denotes the sub-sequence \( (x_{i_1}, x_{i_2}, \ldots, x_{i_k}) \) of \( x^n \). We denote by \( h(\cdot) \) the binary entropy function.

We call a function \( f(n) \geq 0 \) negligible if for any nonzero polynomial \( p(n) \), there exists \( n_0 \) such that

\[
\forall n > n_0, f(n) < 1/p(n).
\]

We call \( f(n) \) overwhelming if \( 1 - f(n) \) is negligible.

C. Non-Signaling Boxes

A non-signaling box is defined by a stochastic matrix

\[
W : \mathcal{U} \times \mathcal{V} \rightarrow \mathcal{X} \times \mathcal{Y}
\]

as follows: Alice gives an input \( u \in \mathcal{U} \) and Bob gives an input \( v \in \mathcal{V} \). Alice gets output \( x \in \mathcal{X} \) and Bob \( y \in \mathcal{Y} \) with probability \( W(xy|uv) \). Furthermore, the following non-signaling conditions must hold

\[
\sum_y W(xy|uv) = \sum_{y'} W(xy|uv') \quad \forall u, v, v', x,
\]

\[
\sum_x W(xy|uv) = \sum_{x'} W(xy|u'v) \quad \forall u, u', v, y,
\]

e.g., the distribution of Alice’s output is independent of Bob’s input (and vice-versa). A party receives its output immediately after giving its input, independently of whether the other has given its input already. Note that this is possible, since the box is non-signaling. Furthermore, after a box is used once, it is destroyed. The set of non-signaling boxes can be divided into two types: local and non-local. A box is local if and only if it can be simulated by non-communicating parties with only shared randomness as a resource. This means that there exist probabilities \( p_i \) and stochastic matrices \( V_A^i, V_B^i \) such that

\[
W(xy|uv) = \sum_{i=1}^n p_i V_A^i(x|u)V_B^i(y|v) \quad \forall u, v, x, y.
\]

A box is called independent if there exist stochastic matrices \( V_A, V_B \) such that

\[
W(xy|uv) = V_A(x|u)V_B(y|v) \quad \forall u, v, x, y,
\]

e.g., such a box can be simulated without any resources at all. In the following we only consider boxes with binary outputs, i.e., \( \mathcal{X} = \mathcal{Y} = \{0, 1\} \). We define

\[
W^A(x|u) := \sum_y W(xy|uv) \quad \forall u, v, x,
\]

\[
W^B(y|v) := \sum_x W(xy|uv) \quad \forall u, v, y.
\]

We call a box with binary outputs perfectly correlated for an input pair \( (u, v) \in \mathcal{U} \times \mathcal{V} \) if

\[
W(01|uv) = W(10|uv) = 0
\]

and perfectly anti-correlated if

\[
W(00|uv) = W(11|uv) = 0.
\]

An input \( u \) for Alice is called redundant if there exists \( \tilde{u} \neq u \) such that

\[
W(xy|uv) = W(xy|\tilde{u}v) \quad \forall x, y, v.
\]

D. Chernoff/Hoeffding Bounds

We will use the following bounds attributed to Chernoff [Che52] and Hoeffding [Hoe63].

**Lemma 1.** Let \( X_1, X_2, \ldots, X_n \) be independent random variables with \( \Pr[X_i = 1] = p_i \) and \( \Pr[X_i = 0] = 1 - p_i \). Let \( X = \sum_{i=1}^n X_i \) and \( \mu = E[X] \). Then for any \( 0 < \delta < 1 \) it holds that

\[
\Pr[X > (1 + \delta)\mu] \leq \exp(-\delta^2\mu/3),
\]

\[
\Pr[X < (1 - \delta)\mu] \leq \exp(-\delta^2\mu/2).
\]

**Lemma 2.** Let \( X_1, X_2, \ldots, X_n \) be independent random variables with \( \Pr[X_i = 1] = p_i \) and \( \Pr[X_i = 0] = 1 - p_i \). Let
Lemma 3. \([\text{MW97}], [\text{RW05}].\) We define \(E.\) Information Theory

\[
X = \sum_{i=1}^{n} X_i \text{ and } \mu = E[X]. \text{ Then for any } 0 < \delta < 1 \text{ it holds that }
\]

\[
\Pr[X > \mu + \delta] \leq \exp(-2\delta^2/n),
\]

\[
\Pr[X < \mu - \delta] \leq \exp(-2\delta^2/n).
\]

E. Information Theory

We will use the smoothed versions of the min-entropy [MW97]. For an event \(E\), let \(P_{X|Y=y}(x)\) be the probability that \(X = x\) and the event \(E\) occurs, conditioned on \(Y = y\). We define

\[
H_{\infty}(X|Y) := \max_{E: \Pr(E) \geq 1-\epsilon} \min_y \min_x (-\log P_{X|Y=y}(x)).
\]

We will make use of the following lemma from [Cac97], [MW97], [RW05].

Lemma 3. Let \(P_{XYZ}\) be a probability distribution. For any \(\epsilon, \epsilon' > 0\),

\[
H_{\infty}^{\epsilon+\epsilon'}(X|YZ) \geq H_{\infty}(XY|Z) - \log(|Y|) - \log(1/\epsilon').
\]

The following lemma from [HR06] gives a lower bound for the smooth entropy of \(n\)-fold product distributions:

Lemma 4. Let \(P_{X^n Y^n} := P_{X_1 Y_1} \ldots P_{X_n Y_n}\) be a probability distribution over \(X^n \times Y^n\) and let \(\epsilon > 0\). Then

\[
H_{\infty}(X^n|Y^n) \geq H(X^n|Y^n) - 4\sqrt{n \log(1/\epsilon') \log(|X|)}.
\]

F. Randomness Extraction and Privacy Amplification

In information-theoretic and quantum key agreement, the final protocol step, where a highly secret key is generated from a longer but only weakly secure key, has been called privacy amplification. It is very closely related to randomness extraction; actually, it corresponds to the latter when viewed from a possible adversary’s perspective.

Definition 1. [CW79] A function \(f: X \times S \rightarrow Y\) is called a 2-universal hash function if for all \(x_0 \neq x_1\) we have

\[
\Pr[f(x_0, S) = f(x_1, S)] \leq \frac{1}{|Y|}
\]

if \(S\) is uniform over \(S\).

Lemma 5 (Leftover hash lemma [BBR88], [ILL89], [BBCN95]). Let \(f : X \times S \rightarrow Y\) be a 2-universal hash function with \(m > 0\). Let \(X\) be a random variable over \(X\) and let \(\epsilon > 0\). If

\[
H_{\infty}(X) - 2\log(1/\epsilon) \geq m,
\]

then \(\frac{1}{2}||(f(S, X), S) - (U, S)||_1 \leq \epsilon\) for \(S\) and \(U\) independent and uniform over \(S\) and \(Y\).

G. Typical Sequences

In this section we will state and prove some basic results on typical sequences. More details on this topic can be found in the book by Csiszár and Körner [CK81].

Definition 2. Let \(P\) be a probability distribution on \(X\) and \(\epsilon > 0\). Then the set of \(\epsilon\)-typical sequences is defined as:

\[
T_{P, \epsilon} := \{x^n \in X^n : \forall x \in X |N(x|x^n) - P(x)| \leq \epsilon n \text{ and } P(x) = 0 \Rightarrow N(x|x^n) = 0\},
\]

where \(N(x|x^n)\) denotes the number of letters \(x\) in \(x^n\).

Definition 3. For a stochastic matrix \(W : X \rightarrow Z\) we define the set of \(W\)-typical sequences under the condition \(x^n \in X^n\) with constant \(\epsilon\) as

\[
T_{W, \epsilon}(x^n) = \{z^n : \forall x, z |N(xz|x^n z^n) - W(z, z) N(x|x^n)| \leq \epsilon n \text{ and } W(z, z) = 0 \Rightarrow N(x|x^n z^n) = 0\}.
\]

The following two well-known lemmas follow directly from Lemma [11].

Lemma 6. \(P^n(T_{P, \epsilon}) \geq 1 - 2|X| \exp(-n\epsilon^2/3)\)

Lemma 7. \(W_{x^n}(T_{W, \epsilon}(x^n)) \geq 1 - 2|X||Z| \exp(-n\epsilon^2/3)\)

Using the results above we will prove a lemma that we will use in the security proofs in this paper. The lemma is similar to Lemma 14 in [WNI03]. Let \(W : X \rightarrow Z\) be a (discrete memoryless) channel, let \(a \in X\) be an input such that the output distribution of \(a\) is not a convex combination of the other output distributions and let \(x^n, \tilde{x}^n \in X^n\) be sequences such that \(|\{k : x_k \neq a\mbox{ and } \tilde{x}_k = a\}| \geq \kappa n\). Then the lemma states that the output of the channel, given \(x^n\) as input, will not be \(W\)-typical conditioned on \(\tilde{x}^n\) with overwhelming probability if \(\exp(-\kappa n)\) is negligible.

Lemma 8. Let \(W : X \rightarrow Z\) be a stochastic matrix and \(a \in X\) such that for all probability distributions \(P\) over \(X\) such that \(P(a) = 0\) and

\[
\left\|W_a - \sum_x P(x) W_x\right\|_1 \geq \delta.
\]

Let \(x^n, \tilde{x}^n \in X^n\) with \(d_H(x^n, \tilde{x}^n) \geq \kappa n\) where \(I_a := \{k : \tilde{x}_k = a\}\). If \(n_a := |I_a| \geq \lambda n\), then

\[
W_{x^n}(T_{W, \epsilon}(\tilde{x}^n)) \leq 2 \exp(-n\epsilon^2/3)
\]

where \(\epsilon := \frac{\lambda \delta}{\sqrt{|Z|}}\).

Proof: Let \(D := \{k \in I_a : x_k \neq \tilde{x}_k\}\). Then it follows that

\[
\left\|\frac{1}{n_a} \sum_{k \in I_a} W_{x_k} - W_a\right\|_1 = \left\|\frac{|D|}{n_a} W_a - \frac{1}{|D|} \sum_{k \in D} W_{x_k}\right\|_1
\]

\[
\geq \frac{|D|}{n_a} \delta \geq \kappa \delta.
\]

This implies that there exists \(b \in Z\) such that

\[
\left\|\frac{1}{n_a} \sum_{k \in I_a} W_{x_k}(b) - W_a(b)\right\| \geq \frac{1}{|Z|} \kappa \delta.
\]
Let \( w^n \in T_{W,\epsilon}(\tilde{x}^n) \). Then it holds that
\[
\left| N(b|w^n) - \sum_{k \in I_a} W_{x_k}(b) \right| = \left| N(ab|\tilde{x}^n w^n) - \sum_{k \in I_a} W_{x_k}(b) \right|
\geq \left| \sum_{k \in I_a} W_{x_k}(b) - n_a W_a(b) \right| - \left| n_a W_a(b) - N(ab|\tilde{x}^n w^n) \right|
\geq \frac{1}{2|Z|} \kappa \delta n_a - \epsilon n
\geq \frac{1}{2|Z|} \kappa \delta n a.
\]

We define independent binary random variables \( X_k, k \in I_a \), with distributions \( P_{X_k}(1) := W_{x_k}(b) \). Let \( X = \sum_{k \in I_a} X_i \) and \( \mu := E[X] = \sum_{k \in I_a} W_{x_k}(b) \). Let \( t := \frac{1}{2|Z|} \kappa \delta \lambda n a \mu^{-1} \) (assuming \( \mu \neq 0 \)). Using the Chernoff bound it follows that
\[
W^n_\epsilon^{\mu}(T_{W,\epsilon}(\tilde{x}^n)) \leq \Pr \left[ |X - \mu| \geq \frac{1}{2|Z|} \kappa \delta \lambda n a \right]
= \Pr \left[ |X - \mu| \geq \epsilon \mu \right]
\leq 2 \exp(-\epsilon^2 n/3).
\]

### III. Impossibility

**Theorem 1.** Let a local non-signaling box with binary output be defined by \( W : U \times V \rightarrow \{0,1\}^2 \) such that
\[
W(xy|uv) = pV^0_A(x|u)V^0_B(y|v) + (1 - p)V^1_A(x|u)V^1_B(y|v)
\]
and there exists \( u_0 \in U, v_0 \in V \) and \( b_0, b_1 \in \{0,1\} \) with:
\[
V^0_A(0|u_0) = V^1_A(1|u_0) = b_0
\]
\[
V^0_A(1|u_0) = V^1_A(0|u_0) = b_0
\]
\[
V^0_B(0|v_0) = V^1_B(1|v_0) = b_1
\]
\[
V^0_B(1|v_0) = V^1_B(0|v_0) = b_0.
\]
then there is no reduction of information-theoretically secure bit commitment to the box \( W \) (with noiseless communication only).

**Proof:** We prove the statement by showing that one can securely implement such a box from noiseless communication and shared randomness alone. This would allow for bit commitment from noiseless communication which is impossible as mentioned above. The implementation just follows the definition of the box: Let \( \lambda \) be the shared random bit. Alice on input \( u \) outputs 0 with probability \( V^0_A(0|u) \) and 1 with probability \( V^1_A(1|u) = 1 - V^0_A(0|u) \). Bob on input \( v \) outputs \( b \in \{0,1\} \) with probability \( V^b_B(b|v) \). This perfectly implements the behavior of the box. Furthermore, this implementation is secure, since Alice and Bob can get the same information (i.e. the shared randomness \( \lambda \)) if they only have black-box access to \( W \), if they always input \( u_0 \) and \( v_0 \), respectively.

### IV. Two Protocols

We will now give two slightly different protocols, which work for two different kinds of non-signaling boxes.

**A. Protocol I**

Informally, the first protocol works as follows: in the Commit protocol an honest Alice gives a fixed input to all her boxes, while Bob chooses his inputs randomly. Alice applies privacy amplification to the outputs of the boxes and uses the resulting key \( K \) to hide the bit \( B \) she wants to commit to. Alice then sends \( K \oplus B \) and the randomness used for privacy amplification to Bob. In the Open protocol Alice sends her outputs from the boxes. Alice’s input is chosen such that there is a statistical test that allows Bob to detect if Alice has changed more than \( O(\sqrt{n}) \) output values while Bob has only limited information about the output of the boxes before the opening phase. A dishonest Alice might still be able to change \( O(\sqrt{n}) \) output values. To ensure that this is not possible, we use a linear code and let Alice send parity check bits of the output to Bob in the Commit protocol. If the minimal distance of the code is large enough, no two strings with the same parity check bits lie in a hamming sphere with radius proportional to \( \sqrt{n} \).

Let Alice and Bob share \( n \) identical non-signaling boxes given by \( W : U \times V \rightarrow \{0,1\}^2 \). In our protocol, we will require Bob to choose his input uniformly from \( V \). For an honest Bob and a potentially malicious Alice, we can define a stochastic matrix \( \tilde{W} : \{0,1\} \times U \rightarrow \{0,1\} \times V \) describing the probability of Bob’s input and output values \( v \) and \( y \), conditioned on Alice’s input \( u \) and output \( x \) as
\[
\tilde{W}(yv|ux) := \frac{1}{|V|} W(xy|uv)\tilde{W}^u(x|u),
\]
if \( W^A(x|u) \neq 0 \), and undefined otherwise. Furthermore, we will require an honest Alice to always input a fixed value \( u_0 \) to the box. For an honest Alice, and a potentially malicious Bob that chooses his input \( v \in \{0,1\} \) freely, we can define random variables \( X_v, Y_v \) depending on Bob’s input that describe the output of Alice and Bob, respectively, i.e. with a joint distribution
\[
P_{X_v,Y_v}(x,y) := W(xy|u_0,v).
\]
The protocol below is secure if there exists a value \( a = (x_a, u_a) \) such that the following condition is fulfilled:

**Condition 1.** (1) There exists \( \delta > 0 \) such that for all probability distributions \( P \) over \( \{0,1\}^2 \) with \( P(a) = 0 \) it holds that
\[
\left\| \tilde{W}_a - \sum_x P(x)\tilde{W}_x \right\|_1 \geq \delta.
\]
(2) There exists \( \gamma > 0 \) such that for all \( v \in V \) it holds that
\[
H(X_v|Y_v) \geq \gamma,
\]
\[\text{i.e., the Shannon entropy of Alice’s output given Bob’s output is non-zero for all possible inputs of Bob.}\]

We will use the labels of Alice as \( \{0,\ldots,|U| - 1\} \). Furthermore, we define the distribution of Alice’s output \( x \) if her input is \( u_a \) as \( P(x) := W^A(x|u_a) \) for all \( x \in \{0,1\} \). Let \( \lambda := \frac{1}{2}\min\{P(x), x \in \{0,1\}\} \). Let \( k \) be the security parameter, \( \epsilon := \frac{1}{2}\lambda k/\sqrt{n} \). Let \( d > 2k \) and let \( H \) be the parity check matrix of a linear \([n, Rn, d]-\)code with \( R > (1 - \gamma)\).
Lemma 9. Let \( l := \gamma n - n(1 - R) - 4\sqrt{nk} - 3k \). We choose \( k := n^{2/3} \), which implies that \( k, \sqrt{nk} \in O(n^{1/6}) \) and \( k, \frac{k^2}{n}, \frac{n^2}{k} \in \Omega(n^{1/3}) \). It follows that \( l \in (\gamma + R - 1)n - O(n^{1/3}) \). If \( n \) is big enough, we have \( l > 0 \). Let \( ext : \{0, 1\}^* \times \{0, 1\}^n \rightarrow \{0, 1\} \) be a 2-universal hash function. We define \( syn(x^n) := H^1(x^n) \).

Commit(b):
- Bob chooses \( v^n \in R \{0, 1\}^n \)
- Alice and Bob input \( u^n \) and \( v^n \) component-wise to the boxes. Alice gets \( x^n \in \{0, 1\}^n \) and Bob \( y^n \in \{0, 1\}^n \).
- Alice chooses \( r \in R \{0, 1\}^* \) and sends \( (syn(x^n), r, b^l \oplus ext(r, x^n)) \) to Bob.

Open():
- Alice sends Bob \( x^n \) and \( b^l \).
- Bob checks:
  - \( syn(x^n) \) is correct
  - \( b \oplus ext(r, x^n) \) is correct
  - \( (y_1, v_1, \ldots, y_n, v_n) \in T^n_{W, x}((x_1, u_a), \ldots, (x_n, u_a)) \)
  - \( x^n \in T^n_{P, x} \)
- If all the checks pass successfully, Bob accepts outputs \( b^l \), otherwise he rejects.

B. Security
Let \( u^n := (u_1, \ldots, u_n) \) be Alice’s input to the boxes, let \( x^n := (x_1, \ldots, x_n) \) be her outputs from the boxes and let \( \tilde{x}^n := (\tilde{x}_1, \ldots, \tilde{x}_n) \) be the values Alice sends to Bob in the opening phase. We define \( z^n := ((x_1, u_1), \ldots, (x_n, u_n)) \) and \( \tilde{z}^n := ((\tilde{x}_1, u_a), \ldots, (\tilde{x}_n, u_a)) \). Let \( r^n := ((y_1, v_1), \ldots, (y_n, v_n)) \) be Bob’s inputs and outputs.

Lemma 9. The protocols Commit and Open satisfy the correctness condition.

Proof: Bob always accepts Commit. If Alice follows the protocol, then \( syn(x^n) \) and \( b^l \oplus ext(r_1, u^n) \) are correct. From Lemma 7 it follows that

\[
Pr[r^n \in T^n_{W, x}(z^n)] = W_{z^n}(T_{W, x}(z^n)) \geq 1 - 16|\mathcal{V}| \exp(-nc^2/3),
\]

and from Lemma 6 it follows that

\[
Pr[x^n \in T^n_{P, x}] = P^n_{x^n}(T_{P, x}) \geq 1 - 4 \exp(-nc^2/3).
\]

Thus, Bob accepts Open with overwhelming probability and outputs \( b^l \), the value Alice was committed to.

Lemma 10. The protocol Commit satisfies the privacy condition with an error negligible in \( n \).

Proof: Let us assume that Alice is honest. Alice inputs \( u_a \) into the boxes as required by the protocol, while Bob can choose its input \( v^n = (v_1, \ldots, v_n) \) freely. We then define the random variables \( X^n = X_{v_1} \times \ldots \times X_{v_n} \) and \( Y^n = Y_{v_1} \times \ldots \times Y_{v_n} \). Let \( \epsilon_1 := 2^{-k} \). According to Lemma 4 it holds that

\[
H_{\infty}^2(X^n|Y^n) \geq H(X^n|Y^n) - 4\sqrt{nk}.
\]

Using Lemma 3 with get that

\[
H_{\infty}^2(X^n|syn(X^n)Y^n) \geq H_{\infty}^2(X^n|Y^n) - n(1 - R) - \log(1/\epsilon_1)
\]

\[
\geq \gamma n - n(1 - R) - 4\sqrt{nk} - k
\]

Thus, Bob accepts with overwhelming probability and outputs \( b^l \), the value Alice was committed to.

Lemma 11. If \( d_H(x^n, \tilde{x}^n) \geq k \), then the probability that Bob accepts \( \tilde{x}^n \) is negligible in \( n \).

Proof: From \( d_H(x^n, \tilde{x}^n) \geq k \) follows \( d_H(z^n, \tilde{z}^n) \geq k \).

Let \( n_a := N(u_a|u^n) \), \( I_a := \{k : z_k = (x_a, u_a)\} \) and \( p := W^A(x_a|u_a) \). For all \( w^n \in T^n_{P, x} \), we have

\[
|N(x_a|u^n) - np| \leq cn = \frac{1}{4}\lambda\delta k/n \cdot n \leq \frac{1}{8}kp,
\]

since \( \lambda \leq p/2 \) and \( \delta \leq 1 \). We distinguish two cases:

\( (1) \ n_a \leq (n - k/2) \): The expectation of \( N((x_a, u_a)|z^n) \) is smaller than or equal to \( (n - \frac{k}{2})p \). Since \( k^2/n \in \Omega(n^{1/3}) \), it follows from Lemma 1 that with overwhelming probability

\[
N((x_a, u_a)|z^n) \leq \left(n - \frac{k}{2}\right)p + \frac{k}{8}p = \left(n - \frac{3k}{8}\right)p.
\]

But since Bob only accepts if \( \tilde{x}^n \in T^n_{P, x} \), we have

\[
d_H(z^n, \tilde{z}^n) \geq \left(n - \frac{k}{4}\right)p - \left(n - \frac{3k}{8}\right)p = \frac{1}{4}kp
\]

and the claim follows from Lemma 8.

\( (2) \ n_a > (n - k/2) \): Then the expectation of \( N((1 - x_a, u_a)|z^n) \) is greater than or equal to \( (n - \frac{k}{2})p \). As \( k^2/n \in \Omega(n^{1/3}) \) Lemma 1 implies that with overwhelming probability

\[
N((1 - x_a, u_a)|z^n) \geq \left(n - \frac{k}{2}\right)(1 - p) - \frac{k}{8}(1 - p) = n(1 - p) - \frac{5}{8}k(1 - p).
\]

But since Bob only accepts if \( \tilde{x}^n \in T^n_{P, x} \), we have

\[
d_H(z^n, \tilde{z}^n) \geq \left(n - \frac{5}{8}k\right)(1 - p) - \left(n - \frac{1}{4}k\right)(1 - p) = \frac{1}{4}k(1 - p)
\]

and the claim follows from Lemma 8.

Lemma 12. The protocol satisfies the binding condition with an error negligible in \( n \).

Proof: Any two strings \( s^n \neq \tilde{s}^n \) with \( syn(s^n) = syn(\tilde{s}^n) \) have distance at least \( d \). So at least one of the two strings has distance at least \( k \) from Alice’s output \( x^n \). The probability that Bob accepts this string in the opening phase is negligible according to lemma 1.
C. Protocol II

Protocol I is not hiding if for every fixed input of Alice a dishonest Bob can choose an input such that he has perfect information about Alice’s output. This is the case for example with the above mentioned NL box. But, as shown in [BCU+06], this box allows for bit commitment. Therefore, we present a second protocol that allows to securely implement bit commitment for such boxes. The protocol works as follows: Alice gives random inputs to all her boxes. Then she applies the protocol to be secure we require that a dishonest Alice cannot change the resulting key to hide the bit she is committed to. In the opening phase Alice sends all her inputs/outputs. Bob performs statistical tests on the output/input of Alice that allow him to detect if Alice has changed more than \( \sqrt{n} \) values. We use again parity check bits of a linear code to make sure that the dishonest Alice cannot change \( \sqrt{n} \) values except with negligible probability.

Alice and Bob share \( n \) identical non-signaling boxes given by \( W : U \times V \rightarrow \{0, 1\}^2 \). We define the corresponding matrix \( \tilde{W} \) as in Section [4.4]. In the following we always assume that \( W_A(x|u) \neq 0 \) for all \( x \in \{0, 1\}, u \in U \). For the following protocol to be secure we require \( \tilde{W} \) to fulfill the following condition:

**Condition 2.** There exist \( u_0, u_1 \in U \), \( u_0 \neq u_1 \), such that the set \( D := \{W_{u_0u_0}, W_{u_1u_1}, W_{u_0u_1}, W_{u_1u_0}\} \) contains at most one non-extreme point of \( \text{conv}(W) \), i.e., there is \( c_0 \in \{u_0u_0, u_1u_1, u_0u_1, u_1u_0\} \) such that for all \( c \in \{u_0u_0, u_1u_1, u_0u_1, u_1u_0\}\{c_0\} \) it holds that for all probability distributions \( P \) with \( P(c) = 0 \)

\[
\left\| \tilde{W} - \sum_z P(z)\tilde{W}_z \right\|_1 \geq \delta.
\]

We label the inputs of Alice as \( \{0, \ldots, |U| - 1\} \) and assume that \( u_0 = 0 \) and \( u_1 = 1 \). In protocol II, we will require Alice to choose her input uniformly from \( \{0, 1\} \) and Bob to choose his input uniformly from \( V \). If both are honest, the joint distribution of the inputs and outputs of Alice and Bob is

\[
P(x, y, u, v) := \begin{cases} \frac{1}{|U|} W(xy|uv), & \text{if } u \in \{0, 1\} \\ 0, & \text{else} \end{cases}
\]

If Alice is honest, the joint distribution of her input and output is

\[
Q(x, u) := \begin{cases} \frac{1}{|U|} W_A(x|u), & \text{if } u \in \{0, 1\} \\ 0, & \text{else} \end{cases}
\]

Let \( \lambda := \frac{1}{|U|} \min\{Q(x, u), (x, u) \in \{0, 1\}^2\} \). Let \( P_0 := \min\{W_A(x|u), (x, u) \in \{0, 1\}^2\} \). Note that we assumed \( P_0 > 0 \) and that obviously we also have \( P_0 \leq \frac{1}{|U|} \). Let \( k_2 \) be the security parameter, \( k_2 := k_1(4P_0 + 1)/2P_0^2 \). \( \epsilon := \frac{1}{4}\lambda k_1/n, d \geq k_1 + 2k_2 + 1, l > 0 \) and let \( H \) be the parity check matrix of a \( n, 2l, d \)-linear code with \( Rn \geq n/2 + 2k_1 + l/2 \). We choose \( k_1 := n^{2/3} \) and \( l := n - 2n(1-R) - 3k_1 \). This implies \( k_1, k_2/n, n/2 \in O(n^{1/3}) \) and \( l \in (2R - 1)n - O(n^{2/3}) \). If \( n \) is big enough, then \( l > 0 \). Let \( \text{ext} : \{0, 1\}^* \times \{0, 1\}^n \rightarrow \{0, 1\}^l \) be a 2-universal hash function.

**Open()**:
- Alice sends Bob \( u^n, x^n \) and \( b' \).
- Bob checks:
  - \( \text{syn}(u^n) \) and \( \text{syn}(x^n) \) are correct
  - \( b' \oplus \text{ext}(r_2, u^n) \) is correct
  - \( ((y_0, y_1), \ldots, (y_{n-1}, y_n)) \in T_{W,\epsilon}((x_0, x_1), \ldots, (x_n, u_n)) \)
  - \( ((x_0, x_1), \ldots, (x_n, u_n)) \in T_{Q,\epsilon} \)
- If all the checks pass successfully, Bob accepts and outputs \( b' \), otherwise he rejects.

**D. Security**

Let \( x^n := ((x_0, x_1), \ldots, (x_n, u_n)) \) be Alice’s input and output, \( z^n := ((\bar{x}_0, \bar{x}_1), \ldots, (\bar{x}_{n-1}, \bar{x}_n)) \) the values Alice sends to Bob in the opening phase and \( r^n := ((y_0, y_1), \ldots, (y_{n-1}, y_n)) \) Bob’s inputs and outputs. For all \( c \in \{0, 1\} \times U \) we define the sets \( I_c := \{i : \bar{z}_i = c\} \).

**Lemma 13.** The protocols Commit and Open satisfy the correctness condition.

**Proof:** Bob always accepts Commit. If Alice follows the protocol, then \( \text{syn}(u^n), \text{syn}(x^n) \) and \( b' \oplus \text{ext}(r_2, u^n) \) are correct. From Lemma [7] it follows that

\[
\Pr[r^n \in T_{W,\epsilon}(z^n)] = \tilde{W}_{z^n}(T_{W,\epsilon}(z^n)) \\
\geq 1 - 8|U||V| \exp(-nc^2/2)
\]

and from Lemma [6] it follows that

\[
\Pr[z^n \in T_{Q,\epsilon}(z^n)] = Q^n(T_{Q,\epsilon}(z^n)) \\
\geq 1 - 4|U| \exp(-nc^2/2) .
\]

Thus, Bob accepts Open with overwhelming probability and outputs \( b' \), the value Alice was committed to.

**Lemma 14.** The protocol Commit satisfies the privacy condition with an error negligible in \( n \).

**Proof:** Let us assume that Alice is honest. Since the box is non-signaling, Bob’s values \( Y^n \) and \( V^n \) are independent of \( U^n \). Since Alice chooses \( U^n \) uniformly from \( \{0, 1\}^n \), we have

\[
H_{\infty}(U^n) = n .
\]

All the information Bob gets about \( U^n \) is \( \text{syn}(U^n) \) and \( \text{syn}(X^n) \). Let \( \epsilon_2 := 2^{-k_1} \). Using Lemma [3] we get

\[
H^n_{\infty}(\text{syn}(U^n)\text{syn}(X^n)) \geq n - 2n(1 - R) - k_1 \\
\geq l + 2k_1 .
\]

If follows from Lemma [5] that extracting \( l \) bits makes the key uniform with an error of at most \( 2\epsilon_2 = 2\cdot2^{-k_1} \). The statement follows.
Lemma 15. If $d_H(z^n, \tilde{z}^n) \geq k_3$, then the probability that Bob accepts $\tilde{z}^n$ is negligible.

Proof: For all $w^n \in T_{Q,e}^n$, it holds that

$$|N(xu|w^n) - nQ(x, u)| \leq cn = \frac{1}{4} \lambda k_1/n \cdot n \leq \frac{1}{64} k_1.$$ 

Since $\lambda \leq \min_{x,u} Q(x,u)/4 \leq 1/16$ and $\delta \leq 1$.

We distinguish the following two cases:

1) There exists $u' \in \{0,1\}$ such that $N(u'|w^n) \leq n/2 - k_1/8$.

For all $x \in \{0,1\}$ the expectation of $N(xu'|z^n)$ is equal to $(n/2 - k_1/8)W_A(x|u')$. Since $k_1/n \in \Omega(n^{-1/3})$ it follows from Lemma 1 that with overwhelming probability

$$N(xu'|z^n) \leq \left(\frac{n}{2} - \frac{1}{8} k_1\right)W_A(x|u') + \frac{1}{16} k_1 W_A(x|u')$$

$$= \left(\frac{n}{2} - \frac{1}{16} k_1\right)W_A(x|u').$$

But since Bob only accepts if $\tilde{z}^n \in T_{Q,e}^n$, we have $d_H(z^I_{\omega'}, \tilde{z}^I_{\omega'}) \geq \frac{1}{16} k_1$ and $d_H(z^I_{\omega'}, \tilde{z}^I_{\omega'}) \geq \frac{1}{16} k_1$, and the claim follows from Lemma 8.

(2) For all $u \in \{0,1\}$ we have $|n/2 - N(u|w^n)| \leq k_1/8$.

Since $z^n \in T_{W_A,x}^n(u^n)$. Assume $z^n \in T_{W_A,x}^n(u^n)$. There exists a value $(x', u') \in \{0,1\}^2$ such that $d_H(z^I_{x',u'}, \tilde{z}^I_{x',u'}) \geq \frac{1}{16} k_1$. Therefore

$$N(x'u'|z^n) + d_H(z^I_{x',u'}, \tilde{z}^I_{x',u'})$$

$$\geq nW_A(x'|u')/2 - k_1 W_A(x'|u')/8 - cn + k_1/4$$

$$\geq nW_A(x'|u')/2 + \frac{1}{64} k_1.$$ 

If there exists $(x'', u'') \neq (x', u') \in \{0,1\}^2$ such that $d_H(z^I_{x'',u''}, \tilde{z}^I_{x'',u''}) \geq \frac{1}{16} k_1$, then the claim follows from Lemma 8. Otherwise $\tilde{z}^n \notin T_{Q,e}^n$.

Next, we will prove a technical lemma:

Lemma 16. For any $n$ it holds that, if $k \leq np$,

$$\sum_{i=0}^{k} \binom{n}{i} p^i(1-p)^{n-i} \leq 2^{-2np^2 + 4pk}.$$ 

Proof: Let $X_1, X_2, \ldots, X_n$ be random variables with $Pr[X_i = 1] = p$ and $Pr[X_i = 0] = (1 - p)$. Let $X = \sum_{i=1}^{n} X_i$. Then using Lemma 2 and setting $t := np - k$,

$$\sum_{i=0}^{k} \binom{n}{i} p^i(1-p)^{n-i} = Pr[X \leq k] \leq \exp(-2t^2/np)$$

$$\leq 2^{-2np^2 + 4pk}.$$ 

Lemma 17. If Alice does not input any values to at least $k_2$ boxes before sending $\text{syn}(x^n)$ to Bob, then Bob does accept the opening of the protocol with negligible probability.

Proof: Alice does not give any input to at least $k_2$ boxes before sending a syndrome $s_0$ to Bob. Later she gives her inputs to the remaining $k_2$ boxes and gets a random output $x_1$ for each box. We know that any two strings $s^n \neq s'^n$ with $\text{syn}(s^n) = \text{syn}(s'^n)$ have distance at least $d > 2k_2$. We can bound the probability that the output string has distance at most $k_1$ to a string with syndrome $s_0$ by

$$\sum_{i=0}^{k_1} \binom{k_2}{i} p_0^i (1 - p_0)^{k_2 - i}.$$ 

Note that since $4p_0 + 1 > 1$ and $2p_0 \leq 1$, we have $p_0 k_2 \geq k_1$.

We can apply Lemma 16 and get an upper bound on this probability of

$$2^{-2k_2 p_0^2 + 4k_1 p_0} = 2^{-2 \frac{k_1 (4p_0 + 1)}{2p_0} - p_0^2 + 4k_1 p_0} = 2^{-k_1}.$$ 

The statement now follows from Lemma 16.

Lemma 18. If Alice changes only $k_1$ values and delays only $k_2$ inputs, then the protocol is binding.

Proof: Any two input strings $s^n$ and $\tilde{s}^n$ with $s_0 = \text{syn}(s^n) = \text{syn}(\tilde{s}^n)$ have distance at least $d$. If we ignore all the positions where Alice did not input anything to the box, $s^n$ and $\tilde{s}^n$ still have distance at least $d - k_2 > 2k_1$.

V. Tightness of Our Results

In this section we show that every non-signaling box with binary outputs that cannot be securely implemented from shared randomness allows to realise bit commitment with one of the above protocols.

Lemma 19. Let $W : \mathcal{U} \times \mathcal{V} \rightarrow \{0,1\}^2$ be a non-signaling box with $|\mathcal{U}| \geq 2$. If there exists $(x_0, u_0)$ such that either $W(x_0|u_0) = 0$ or $W(x_0|u_0) = W_{x_0|u_0}$ for some $(x_1, u_1) \neq (x_0, u_0)$ with $W(x_0|u_0) \leq W(x_1|u_1)$, then bit commitment can be implemented from $W$ if and only if bit commitment can be implemented from the reduced box $W$ that is obtained by removing input $u_0$ from $W$. Furthermore, $W$ is local if and only if $W$ is local.

Proof: We proof the statement by showing that Alice having access to $W$ can simulate the behavior of $W$ on input $u_0$ using local randomness: We first consider the case where $W_{x_0|u_0} = W_{x_1|u_1}$, with $u_1 \neq u_0$ and $W(x_1|u_1) \neq 0$. We define $p := W(x_0|u_0)/W(x_1|u_1)$. Then it holds that

$$W(x_0 y|u_0 v) = p W(x_1 y|u_1 v)$$

for all $y \in \{0,1\}, v \in \mathcal{V}$. It follows from the non-signaling conditions that

$$W((1-x_0)y|u_0 v) = (1-p)W(x_1 y|u_1 v) + W((1-x_0)y|u_1 v)$$

for all $y \in \{0,1\}, v \in \mathcal{V}$. We assume $x_0 = x_1 = 0$. Then we can simulate $W$ using $W$ in the following way: Alice gives input $u_0$ to $W$ and gets output $x$. If $x = 1$, then Alice outputs

$$1.$$ 

If $x = 0$, then Alice outputs 0 with probability $p$ and 1 with
probability $1 - p$. If $W^A(x_0|u_0) = 0$ or $\hat{W}_{\text{l}u_0} = \hat{W}_{\text{l}u_1}$, then Alice on input $u_0$ outputs 0 with probability $W^A(0|u_0)$ and 1 with probability $W^A(1|u_0)$.

Theorem 2. A non-signaling box $W : \{0,1\}^2 \rightarrow \{0,1\}^2$ that fulfills neither Condition $\mathbb{E}$ nor Condition $\mathbb{F}$ does not allow for information-theoretically secure bit commitment (with noiseless communication only) and is local.

Proof: We first consider the case where there exists $(x_0, u_0)$ such that $W^A(x_0|u_0) = 0$ or $\hat{W}_{\text{l}u_0} = \hat{W}_{\text{l}u_1}$ for some $(x_1, u_1) \neq (x_0, u_0)$. We assume $W^A(x_0|u_0) \leq W^A(x_1|u_1)$ and examine the box $\hat{W}$ that is obtained by removing input $u_0$. $\hat{W}$ is obviously local. If $\hat{W}(0|u_1) = \hat{W}(1|u_1)$, the box is independent and doesn’t allow for bit commitment. If there is a perfectly correlated or anti-correlated input pair, the box doesn’t allow for bit commitment according to Theorem $\mathbb{I}$. Otherwise bit commitment can be reduced to this box using Protocol $\mathbb{I}$. From Lemma $\mathbb{I}$ it follows that we can implement bit commitment from $\hat{W}$ if and only if bit commitment can be implemented from $W$. Thus, the claim follows for all boxes with $W^A(x|u) = 0$ or $\hat{W}_{\text{l}u} = \hat{W}_{\text{l}u_1}$ for some $(x_1, u_1) \neq (x_0, u_0)$. In the following we assume $W^A(x_0|u_0) = 0$ for all $x_0, u_0 \in \{0,1\}$ and $\hat{W}_{\text{l}u} = \hat{W}_{\text{l}u_1}$ for all $z, z' \in \{0,1\}^2$ with $z \neq z'$.

(1) $|\text{extr}(\text{conv}(W))| \geq 3$: Then the box fulfills Condition $\mathbb{I}$ and we can securely implement bit commitment using Protocol $\mathbb{I}$.

(2) $|\text{extr}(\text{conv}(\hat{W}))| = 2$: We first consider the case $\hat{W}_{\text{l}u}, \hat{W}_{\text{l}u_0} \in D$. Without loss of generality, we can assume $u = 0$. Then there exist $0 < \lambda_0, \mu_0 < 1$ such that

$$\hat{W}_{01} = \lambda_0 \hat{W}_{00} + (1 - \lambda_0) \hat{W}_{10},$$

and

$$\hat{W}_{11} = \mu_0 \hat{W}_{00} + (1 - \mu_0) \hat{W}_{10}.$$ 

We define $\lambda_1 := 1 - \lambda_0$ and $\mu_1 := 1 - \mu_0$. Then it follows from the non-signaling conditions that for all $(y, v) \in \{0,1\} \times V$

$$\frac{W(0y|1v)}{W^A(0|1)} = \frac{\lambda_0 W(0y|0v)}{W^A(0|0)} + \frac{\lambda_1 W(1y|0v)}{W^A(1|0)},$$

$$\frac{W(1y|1v)}{W^A(1|1)} = \frac{\mu_0 W(0y|0v)}{W^A(0|0)} + \frac{\mu_1 W(1y|0v)}{W^A(1|0)}.$$ 

We define

$$a_x := \frac{\lambda_x W^A(0|1)}{W^A(x|0)}, \quad x \in \{0,1\},$$

and

$$b_x := \frac{\mu_x W^A(1|1)}{W^A(x|0)}, \quad x \in \{0,1\}.$$ 

Then it follows from the non-signaling conditions that for all $(y, v) \in \{0,1\} \times V$ it holds that $W(0y|0v) + W(1y|0v)$ is equal to

$$(a_0 + b_0)W(0y|0v) + (a_1 + b_1)W(1y|0v)$$

As we have excluded the case $\hat{W}_{10} = \hat{W}_{00}$, it follows that $a_0 + b_0 = a_1 + b_1 = 1$. Then the box is local as follows from $W(x|y) = W^A(0|0) V^A_A(x|u) V^A_B(y|v) + W^A(1|0) V^A_A(x|u) V^A_B(y|v)$ with

| $(x, u)$ | $V^A_A(x|u)$ | $V^A_B(y|v)$ |
|----------------|----------------|----------------|
| $(0,0)$ | $a_0$ | $0$ |
| $(0,1)$ | $a_1$ | $b_1$ |
| $(1,0)$ | $b_0$ | $0$ |
| $(1,1)$ | $b_1$ | $a_1$ |

and

$$V^A_B(y|v) := W(0y|0v)/W^A(0|0),$$

$$V^A_B(y|v) := W(1y|0v)/W^A(1|0)$$

for all $y, v \in \{0,1\}$. If one of the inputs $(0,0)$ or $(0,1)$ is perfectly correlated or anti-correlated, then we cannot reduce bit commitment to this box (Theorem $\mathbb{I}$). Otherwise we can securely implement bit commitment from this box using Protocol $\mathbb{I}$.

Next, we consider the case $\hat{W}_{x0} = \hat{W}_{x'} \in D$, $x, x' \in \{0,1\}$. We assume $x = x' = 0$. Then it holds that

$$\hat{W}_{10} = \lambda_0 \hat{W}_{00} + \lambda_0 \hat{W}_{01},$$

and

$$\hat{W}_{11} = \mu_0 \hat{W}_{00} + \mu_1 \hat{W}_{01}.$$ 

If there is $u \in \{0,1\}$ such that for all $v \in \{0,1\}$ the box is neither perfectly correlated nor perfectly anti-correlated for input $(u, v)$, then the box fulfills Condition $\mathbb{I}$. Otherwise, there must be $v_0, v_1 \in \{0,1\}$ such that the box is perfectly correlated or anti-correlated for both $(0, v_0)$ and $(1, v_1)$. Then it follows that $\lambda_0 = 0$ and $\mu_0 = 0$, which is a contradiction to our assumptions.

The case $|\text{extr}(\text{conv}(\hat{W}))| \leq 1$ we have already excluded.

In order to prove that we can reduce bit commitment to any box with binary outputs (and general input alphabets $\mathcal{U}$ and $\mathcal{V}$) that cannot be securely implemented from shared randomness we need to give an alternative condition for the security of Protocol $\mathbb{II}$.

Condition 3. There exist $u_0, u_1 \in \mathcal{U}$, $u_0 \neq u_1$ and $x_0, x_1 \in \{0,1\}$ such that the following two conditions hold:

(1) $W_{x_0 u_0}, W_{x_1 u_1}$ are extreme points of $\text{conv}(W)$, i.e., for all $c \in \{(x_0, u_0), (x_1, u_1)\}$ it holds that for all probability distributions $P$ s.t. $P(c) = 0$

$$\left\|W_c - \sum_z P(z)W_z\right\|_1 \geq \delta.$$ 

(2) Let $c, c' \in \{(1 - x_0, u_0), (1 - x_1, u_1)\}$ with $c \neq c'$. Then for all probability distributions $P$ such that $P(c') > 0$ and $P(c) = 0$ it holds that

$$\left\|W_c - \sum_z P(z)W_z\right\|_1 \geq \delta.$$ 

To prove Protocol $\mathbb{II}$ secure for all boxes that fulfill Condition $\mathbb{I}$ we replace Lemma $\mathbb{I}$ with the following lemma. We assume that $(x_0, u_0) = (0,0)$ and $(x_1, u_1) = (0,1)$.

Lemma 20. If $d_H(z^n, \tilde{z}^n) \geq k_1$, then the probability that Bob accepts $\tilde{z}^n$ is negligible in $n$.

Proof: For all $w^n \in T_{Q, \epsilon}$ it holds that $|N(xuw^n) - \frac{n}{2} W^A(x|u)| \leq cn \leq \frac{1}{12} k_1$. We distinguish the following two cases:
(1) If there exists \( w' \in \{0, 1\} \) such that \( N(w'|w^n) \leq n/2 - k_1/8 \), then the statement follows from the proof of Lemma 15. 

(2) If \( 2 - N(u|w)| \leq k_1/8 \) for all \( u \in \{0, 1\} \), then it follows from Lemma 7 that with overwhelming probability \( z^n = 1 \). Assume without loss of generality that \( W \). 

Then there exist \( \lambda_{z_1} \) with \( \sum_{z \in D} \lambda_z W_z = 1 \) such that \( W_{(1-x_0)u_0} = \sum_{z \in D} \lambda_z W_z \). 

There exists \((x_1, u_1)\) with \( u_1 \neq u_0 \) such that \( \lambda_{x_1u_1} > 0 \). We assume \( x_0 = x_1 = 1 \). We have \( W_{(0)u_0} = 0 \). This implies \( W_{(0)u_0} = 0 \). From the non-signaling conditions follows that \( W_{(0)u_0} = W_{(0)u_0} > 0 \). This exists \( v_1 \in V \) such that \((u_1, v_1)\) is perfectly correlated or anti-correlated. We assume without loss of generality that \( (u_1, v_1) \) is perfectly correlated. This implies \( W_{(0)u_1v_1} > 0 \) and \( W_{(1)u_1v_1} = 0 \). From \( \lambda_{x_1u_1} > 0 \) follows that \( W_{(0)u_1v_1} > 0 \). So we have \( W_{u_0}, W_{u_1} \in D, W_{(0)u_0} = W_{(0)u_1} = W_{(1)u_0} = W_{(1)u_1} > 0 \). Thus, Condition 5 is fulfilled. 

VI. Concluding Remarks

We have shown that any non-signaling two-partite system with binary outputs can either be realized by shared randomness or allows for bit commitment. This all-or-nothing result implies, in particular, that the classical measurement-outcome behavior of a two-qubit state can be used for bit commitment if it has no hidden-variable explanation.

Obvious challenging open questions are whether a similar result holds for arbitrary output alphabets. Furthermore, it would be interesting to know under what circumstances (the stronger functionality of) oblivious transfer can be obtained. In certain settings, e.g., distributed information or noisy channels, bit commitment and oblivious transfer have turned out to be realizable from exactly the same starting points.

References

[BBCM95] C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer. Generalized privacy amplification. IEEE Transactions on Information Theory, 41, 1995.

[BRR88] C. H. Bennett, G. Brassard, and J.-M. Robert. Privacy amplification by public discussion. SIAM Journal on Computing, 17(2):251–299, 1988.

[BCU+06] H. Buhrman, M. Christandl, F. Unger, S. Wehner, and A. Winter. Implications of superstrong nonlocality for cryptography. Proceedings of the Royal Society A, 462:1919–1932, 2006.

[Bu83] M. Blum. Coin flipping by telephone a protocol for solving impossible problems. SAGA News, 15(1):23–25, 1983.

[Cac97] C. Cachin. Entropy Measures and Unconditional Security in Cryptography. PhD thesis, ETH Zurich, Switzerland, 1997.

[Che52] H. Chernoff. A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations. Annals of Mathematical Statistics, 23:493–507, 1952.

[CRIK81] I. Csiszár and J. Körner. Information Theory: Coding Theorems for Discrete Memoryless Systems. Academic Press, New York, 1981.

[Cre97] C. Crépeau. Efficient cryptographic protocols based on noisy channels. In Advances in Cryptology — CRYPTO ’97, volume 1233 of Lecture Notes in Computer Science, pages 306–317. Springer-Verlag, 1997.

[CW79] J. L. Carter and M. N. Wegman. Universal classes of hash functions. Journal of Computer and System Sciences, 18:143–154, 1979.

[Hoe63] W. Hoeffding. Probability inequalities for sums of bounded random variables. Journal of the American Statistical Association, 58(301):13–30, 1963.

[HR06] T. Holenstein and R. Renner. On the randomness of independent experiments. http://arxiv.org/, cs.IT/0608007, 2006.

[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.

[IMNW06] H. Imai, K. Morozov, A. C. A. Nascimento, and A. Winter. Efficient protocols achieving the commitment capacity of noisy correlations. Information Theory, 2006 IEEE International Symposium on, pages 1432–1436, 2006.

[IMQNW04] H. Imai, J. Müller-Quade, A. Nascimento, and A. Winter. Rates for bit commitment and coin tossing from noisy correlation. In Proceedings of the IEEE International Symposium on Information Theory (ISIT’04), 2004.

[LC97] H. K. Lo and H. F. Chau. Is quantum bit commitment really possible? Physical Review Letters, 78:3410–3413, 1997.

[May97] D. Mayers. Unconditionally secure quantum bit commitment is impossible. Physical Review Letters, 78:3414–3417, 1997.

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

[PR97] S. Popescu and D. Rohrlich. Causality and nonlocality as axioms for quantum mechanics. In Proceedings of the symposium on Causality and Locality in Modern Physics and Astronomy: Open Questions and Possible Solutions, 1997. Also available at http://arxiv.org/abs/quant-ph/9709026.

[RW04] R. Renner and S. Wolf. Smooth renyi entropy and applications. In Proceedings of 2004 IEEE International Symposium on Information Theory (ISIT’04), page 233, 2004.
[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 Lecture Notes in Computer Science, pages 199–216. Springer-Verlag, 2005.

[SGP05] T. Short, N. Gisin, and S. Popescu. The physics of no-bit-commitment: generalized quantum non-locality versus oblivious transfer. http://arxiv.org/abs/quant-ph/0508120, 2005.

[WNI03] A. Winter, A. C. A. Nascimento, and H. Imai. Commitment capacity of discrete memoryless channels. In IMA Int. Conf., pages 35–51, 2003.

[WW04] S. Wolf and J. Wullschleger. Zero-error information and applications in cryptography. In Proceedings of 2004 IEEE Information Theory Workshop (ITW ’04), 2004.

[WW05a] S. Wolf and J. Wullschleger. Bit commitment from weak non-locality. In Proceedings of 2005 IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, 2005.

[WW05b] S. Wolf and J. Wullschleger. Oblivious transfer and quantum non-locality. In Proceedings of the IEEE International Symposium on Information Theory (ISIT ’05), 2005.