The role of help in Classical and Quantum Zero-Knowledge

André Chailloux*
LRI
Université Paris-Sud
andre.chailloux@ens-lyon.org

Iordanis Kerenidis*
CNRS - LRI
Université Paris-Sud
jkeren@lri.fr

November 9, 2007

Abstract

We study the role of help in Non-Interactive Zero-Knowledge protocols and its relation to the standard interactive model. In the classical case, we show that help and interaction are equivalent, answering an open question of Ben-Or and Gutfreund ([BG03]). This implies a new complete problem for the class SZK, the Image Intersection Density. For this problem, we also prove a polarization lemma which is stronger than the previously known one.

In the quantum setting, we define the notion of quantum help and show in a more direct way that help and interaction are again equivalent. Moreover, we define quantum Non-Interactive Zero-Knowledge with classical help and prove that it is equal to the class of languages that have classical honest-Verifier Zero Knowledge protocols secure against quantum Verifiers ([Wat06, HKSZ07]). Last, we provide new complete problems for all these quantum classes.

Similar results were independently discovered by Dragos Florin Ciocan and Salil Vadhan.

*Supported in part by ACI Securité Informatique SI/03 511 and ANR AlgoQP grants of the French Ministry and in part by the European Commission under the Intergrated Project Qubit Applications (QAP) funded by the IST directorate as Contract Number 015848.

1 Introduction

In the setting of Zero-Knowledge, the Prover can prove to the Verifier that the answer to an instance of a problem, e.g. an NP problem with a witness w, is Yes without giving any other information. In particular, the person that receives the proof does not learn anything about w or any other witness. In order to create this kind of proofs, the Prover and the Verifier interact with each other. The condition "without giving any other information" has been formalized in [GMR89, GMW91] and this security condition has been defined in the computational and the information-theoretic setting.

We are interested in the information-theoretic setting and the class SZK (Statistical Zero-Knowledge) where an exponentially small amount of information is leaked. This class has been widely studied and many properties thereof are known (eg. [Oka96, Vad99]). Some non-interactive models have also been defined where there is a single message from the Prover to the Verifier. If the Prover and Verifier do not share anything in the beginning of the protocol, then the resulting class is no larger than BPP. However, we can enhance the model, either by having the Prover and Verifier share a uniformly random string (the $NISZK$ class, see [DMP88], [GSV99]) or some limited trusted help (the $NISZK_{|h}$ class).

The class $NISZK_{|h}$ was introduced by Ben-or and Gutfreund [GB00]. In this setting, the Prover and Verifier receive in the beginning of the protocol some help from a trusted third party, the *Dealer*. The Dealer has polynomial power, hence the help is "limited", however he knows the input to the problem. They showed that help does not add anything if we allow interaction ($SZK = SZK_{|h}$). They also described a complete problem for the class $NISZK_{|h}$, the Image Intersection Density (IID), and showed that $NISZK \subseteq NISZK_{|h} \subseteq SZK$, in other words that help can always be replaced by interaction. They also claimed to prove the opposite inclusion, $SZK \subseteq NISZK_{|h}$, however they later retracted from this claim ([BG03]).

In this paper, we start by proving that indeed help and interaction are equivalent in Zero-Knowledge proofs, i.e. $SZK = NISZK_{|h}$ (Section 4). Our result can be thought of as showing that the power of SZK lies only in the fact that there is a trusted access to the input (from the Verifier or from the Dealer). It will hopefully provide some more insight into the relation between the classes $NISZK$ and SZK, which is a main open question in the area. Moreover, we show that the IID problem remains complete for a wider range of parameters. For the proof we use a polarization lemma that is based on new bounds on the Statistical Difference problem (Appendix A).

In 2002, Watrous defined a quantum analog of Zero-Knowledge proofs ([Wat02]) and studied the quantum class $QSZK$. Since then, there has been a series of works that deal with the power and limitations of quantum Zero-Knowledge proofs ([Kob03, Wat06, Kob07]) as well as attempts to find classical interactive protocols that remain zero-knowledge even against quantum adversaries ([Wat06, HKSZ07]).

In the second part of our paper, we start by studying the class $QNISZK$ that was defined by Kobayashi in [Kob03]. Using new results from [BT07], we give two complete problems for this class, the Quantum Entropy Approximation (QEA) and the Quantum Statistical Closeness to Uniform ($QSCU$). These complete problems are the quantum equivalents of the complete problems for $NISZK$. However, due to the fact that quantum expanders are different than classical ones, the proof is different than in the classical case (Section 5).

In addition, we study the role of help in quantum Zero-Knowledge protocols. We define the notion of quantum help and show in a straightforward way that it is again the case that help and interaction are equivalent. We also define quantum Zero-Knowledge with classical help, provide a complete problem for the class and deduce that the message of the Prover can also be classical. This allows us to prove that this class is equivalent to the class of languages that have classical interactive protocols that remain zero-knowledge even against quantum honest Verifiers (Section 6).

2 Preliminaries

We start by describing some operations on probability distributions and proceed to provide definitions for classical and quantum Zero Knowledge classes and their complete problems.

2.1 Operations on Probability distributions

Let $X : \{0,1\}^n \rightarrow \{0,1\}^m$ be a polynomial size circuit. The distribution encoded by X is the distribution induced on $\{0,1\}^m$ by evaluating X on a uniformly random input from $\{0,1\}^n$. We abuse notation and denote this distribution by X, in other words, X is both a circuit that encodes a distribution and the distribution itself. Also, $\mathcal{P}_n$ is the set of probability distributions on $\{0,1\}^n$.

Denote by $SD(X,Y)$ the Statistical Difference between X and Y, $SC(X,Y)$ their Statistical Closeness, $Disj(X,Y)$ the Disjointness of X according to Y and mut-$Disj$ the mutual Disjointness between X and Y.

- $SD(X,Y) = \frac{1}{2}\sum_i |x_i - y_i| = 1 - \sum_i \min(x_i, y_i)$
- $SC(X,Y) = 1 - SD(X,Y) = \sum_i \min(x_i, y_i)$
- $Disj(X,Y) = \frac{1}{2^n}|\{i \in \{0,1\}^n \mid \forall j \in \{0,1\}^n,\ X(i) \neq Y(j)\}$
- mut -$Disj(X,Y) = min(Disj(X,Y), Disj(Y,X))$

Note that $Disj(X,Y) \leq SD(X,Y)$ and that $Disj(X,Y) \neq Disj(Y,X)$ but mut-$Disj(X,Y)$ =mut-$Disj(Y,X)$.

Tensor Product $X \otimes Y$ corresponds to the distribution (X,Y). If $X \in \mathcal{P}_n$ and $Y \in \mathcal{P}_m$ then $X \otimes Y \in \mathcal{P}_{n+m}$. We denote $X^{\otimes k}$ the distribution that results by tensoring X k times.

Prop 1 (Direct Product Lemmas). *Let X, Y any probability distributions. Then,*

1. $SD(X,Y) = \delta \implies 1 - 2\exp^{-k\delta^2/2} \leq SD(X^{\otimes k}, Y^{\otimes k}) \leq k\delta$
2. $Disj(X,Y) = \delta \implies Disj(X^{\otimes k}, Y^{\otimes k}) = 1 - (1-\delta)^k$

XORing Distributions We define the XOR operator which acts on a pair of distributions and returns a pair of distributions. Let $(A,B) = XOR(X_0, X_1)$. Then,

$$A : \text{pick } b \in_R \{0,1\}, \text{return a sample of } X_b \otimes X_b$$
$$B : \text{pick } b \in_R \{0,1\}, \text{return a sample of } X_b \otimes X_{\bar{b}}$$

Prop 2 (XOR Lemmas). *Let X, Y probability distributions and $(A,B) = XOR(X,Y)$. Then,*

1. $SD(X,Y) = \delta \implies SD(A,B) = \delta^2$
2. *mut-$Disj(X,Y) = \delta \implies$ mut-$Disj(A,B) = \delta^2$*

Flat Distributions Let X a distribution with entropy $H(X)$. Elements x_i of X such that $|\log(x_i) + H(X)| \leq k$ are called k-typical. We say that X is Δ-flat if for every $t > 0$ the probability that an element chosen from X is $t \cdot \Delta$-typical is at least $1 - 2^{-t^2+1}$.

Prop 3 (Flattening Lemma). *Let $X : \{0,1\}^n \to \{0,1\}^m$ a circuit that encodes a distribution. Then $X^{\otimes k}$ is $\sqrt{k} \cdot n$-flat.*

2-Universal hashing functions A family $\mathcal{H}$ of 2-Universal hashing functions from $A \to B$ is such that for every two elements $x, y \in A$ and $a, b \in B$ $Pr_{h \in_R \mathcal{H}}[\ h(x) = a \text{ and } h(y) = b] = \frac{1}{|B|^2}$.

Prop 4 (Leftover hash lemma). *Let $\mathcal{H}$ a samplable family of 2-Universal hashing functions from $A \to B$. Suppose X is a distribution on A such that with probability at least $1 - \delta$ over x selected from X, $Pr[X = x] \leq \epsilon/|B|$. Consider the following distribution*

$$Z : \textit{choose } h \leftarrow \mathcal{H} \textit{ and } x \leftarrow X.\ \textit{return } (h, h(x))$$

Then, $SD(Z, I) \leq O(\delta + \epsilon^{1/3})$, where I is the Uniform distribution on $\mathcal{H} \times B$.

2.2 Classical Zero Knowledge

Zero Knowledge proofs are a special case of interactive proofs. Here, we also want that the Verifier learns nothing from the interaction other than the fact that $x \in \Pi_Y$ when it is the case. The way it is formalized is that for $x \in \Pi_Y$, the Verifier can simulate his view of the protocol defined by all the messages sent during the protocol as well as the verifier's private coins.

Definition 1. *$\Pi \in SZK$ iff there exists an interactive protocol $\langle P, V \rangle$ that solves Π such that there exists a function S computable in polynomial time and a function $\mu \in negl(k) \ll 1/poly(k)$ that has the following property :*

$$\forall x \in \Pi_Y,\ SD\left(S(x, 1^k), \langle P, V \rangle_V\right) \leq \mu(k)$$

S is called the simulator. We also have the following non-interactive variants of SZK:

• **NISZK** : We suppose here that the Prover and the Verifier additionally share a truly random string r. We want the Verifier to be able to simulate both the random string and the message m_P from the Prover on Yes instances.

Definition 2. *$\Pi \in NISZK$ iff with a truly random shared string r, there exists an non-interactive protocol $\langle P, V \rangle$ that solves Π such that there exists a function S computable in polynomial time and a function $\mu \in negl(k) \ll 1/poly(k)$ that has the following property :*

$$\forall x \in \Pi_Y,\ SD\left(S(x, 1^k), (r, m_P(r, x))\right) \leq \mu(k)$$

• $\mathbf{NISZK_{|h}}$: We suppose here that the Prover and the Verifier additionally share a string h that is generated by a trusted third party (the dealer) using some coins unknown to the verifier and the prover. This string is called the help and can depend on the input. We want the Verifier to be able to simulate both the help and the Prover's message on Yes instances.

Definition 3. *$\Pi \in NISZK_{|h}$ iff there exists a non-interactive protocol $\langle D, P, V \rangle$ that solves Π where :*

- *The prover and the verifier share some help h which is a random sample of D depending on the input.*
- *There exists a function S computable in polynomial time and a function $\mu \in negl(k) \ll 1/poly(k)$ that has the following property :*

$$\forall x \in \Pi_Y, \ SD\left(S(x, 1^k), (h, m_P(h, x))\right) \leq \mu(k)$$

2.3 Quantum Statistical Zero Knowledge

Quantum Statistical Zero Knowledge proofs are a special case of Quantum Interactive Proofs. We can think of a quantum interactive protocol $\langle P, V\rangle(x)$ as a circuit $(V_1(x), P_1(x), \ldots, V_k(x), P_k(x))$ acting on $\mathcal{V} \otimes \mathcal{M} \otimes \mathcal{P}$. $\mathcal{V}$ are the Verifier's private qubits, $\mathcal{M}$ are the message qubits and $\mathcal{P}$ are the Prover's private qubits. $V_i(x)$ (resp. $P_i(x)$) represents the i^{th} action of the Verifier (resp. the Prover) during the protocol and acts on $\mathcal{V} \otimes \mathcal{M}$ (resp. $\mathcal{M} \otimes \mathcal{P}$). β_i corresponds to the state that appears after the i^{th} action of the protocol.

In the Zero-Knowledge setting, we also want that the Verifier learns nothing from the interaction other than the fact that $x \in \Pi_Y$ when it is the case. The way it is formalized is that for $x \in \Pi_Y$, the Verifier can simulate his view of the protocol. We are interested only in protocols where the Verifier and the Prover use unitary operations.

Let $\langle P, V\rangle$ a quantum protocol and β_j defined as before. The Verifier's view of the protocol is his private qubits and the message qubits. $view_{\langle P,V\rangle}(j) = Tr_{\mathcal{P}}(\beta_j)$. We also want to separate the Verifier's view whether the last action was made by the Verifier or the Prover. We note ρ_0 the input state, ρ_i the Verifier's view of the protocol after P_i and ξ_i the Verifier's view of the protocol after V_i.

We say that the Verifier's view can be simulated if on an input x, there is a negligible function μ such that $\forall j$ we can create σ_j with quantum polynomial computational power such that

$$\|\sigma_j - view_{V,P}(j)\| \leq \mu(|x|)$$

Note that for a state σ such that $\|\sigma - \rho_i\| \leq \mu(|x|)$ it is easy to see that $\sigma' = V_{i+1}\sigma V_{i+1}^\dagger$ is close to $\xi_{i+1} = V_{i+1}\rho_i V_{i+1}^\dagger$ in this sense that $\|\sigma' - \xi_{i+1}\| \leq \mu(|x|)$. Therefore we just need to simulate the ρ_i's.

Definition 4. *A protocol $\langle P, V\rangle$ has the zero-knowledge property for Π if for each input $x \in \Pi_Y$, there is a negligible function μ such that $\forall j$ we can create σ_j with quantum polynomial computational power such that*

$$\|\sigma_j - \rho_j\| \leq \mu(|x|)$$

This formalizes the fact that on Yes instances, the Verifier does not learn anything from the protocol except the fact that the input is a Yes instance.

Definition 5. $\Pi \in QSZK$ *iff there exists a quantum protocol $\langle P, V\rangle$ that solves Π and that has the zero-knowledge property for Π.*

In the setting of Quantum Non-Interactive Statistical Zero-Knowledge, first defined by Kobayashi [Kob03], the Prover and Verifier share a maximally entangled state $\sum_i |i\rangle|i\rangle$ and then the Prover sends a single quantum message to the Verifier.

Definition 6. $\Pi \in QNISZK$ *iff, when the Prover and Verifier share the maximally entangled state* $\sum_i |i\rangle|i\rangle$, *there exists a quantum non-interactive protocol* $\langle P, V\rangle$ *that solves* Π *and that has the zero-knowledge property for* Π.

The notion of quantum help is more intricate and will be the subject of Section 6.

2.4 Complete problems for Zero-Knowledge classes

The complete problems for the Zero-Knowledge classes are promise problems. A promise problem Π is defined by two disjoint sets Π_Y and Π_N. An instance X of Π is an element of $\Pi_Y \cup \Pi_N$. We say that Π reduces to Ω ($\Pi \preccurlyeq \Omega$) iff there exists a poly-time computable function f such that

$$X \in \Pi_Y \;\Rightarrow\; f(X) \in \Omega_Y \text{ and } X \in \Pi_N \;\Rightarrow\; f(X) \in \Omega_N$$

If $\Pi \preccurlyeq \Omega$ then Π is no-harder than Ω. We can define the complement problem $\overline{\Pi}$ as follows : $\overline{\Pi}_Y = \Pi_N$ and $\overline{\Pi}_N = \Pi_Y$. In what follows, X, Y are circuits encoding probability distributions.

SZK-complete problems :

Statistical Difference **(SD)** ***Entropy Difference*** **(ED)**

$(X,Y) \in SD_Y \Rightarrow SD(X,Y) \geq 2/3$ $\quad (X,Y) \in ED_Y \Rightarrow H(X) - H(Y) \geq 1$
$(X,Y) \in SD_N \Rightarrow SD(X,Y) \leq 1/3$ $\quad (X,Y) \in ED_N \Rightarrow H(Y) - H(X) \geq 1$

$NISZK$-complete problems :

Entropy Approximation **(EA^t)** ***Statistical Closeness to Uniform*** **(SCU)**

$X \in EA^t_Y \Rightarrow H(X) \geq t+1$ $\quad X \in SCU_Y \Rightarrow SD(X,I) \leq 1/n$
$X \in EA^t_N \Rightarrow H(X) \leq t-1$ $\quad X \in SCU_N \Rightarrow SD(X,I) \geq 1 - 1/n$

$NISZK_{|h}$-complete problem :

Image Intersection Density **(IID)**

$(X,Y) \in IID_Y \Rightarrow SD(X,Y) \leq 1/n^2$
$(X,Y) \in IID_N \Rightarrow Disj(X,Y) \geq 1 - 1/n^2$

Let us also define another problem related to IID which is not complete:

Mutual Image Intersection Density **(mut-IID)**

$(X,Y) \in \text{mut-}IID_Y \Rightarrow SD(X,Y) \leq 1/n^2$
$(X,Y) \in \text{mut-}IID_N \Rightarrow \text{mut-}Disj(X,Y) \geq 1 - 1/n^2$

Note that we can change the parameters to other parameters α and β. For example, $SD^{\alpha,\beta}$ corresponds to : $(X,Y) \in SD^{\alpha,\beta}_Y \implies SD(X,Y) \geq \alpha$ and $(X,Y) \in SD^{\alpha,\beta}_N \implies SD(X,Y) \leq \beta$

Similarly, we can define the quantum equivalent problems QSD, QED, QEA^t and $QSCU$. In this case, X, Y are the density matrices that correspond to the output qubits of the circuits, $SD(X,Y)$ is the trace distance and the entropy is the von Neumann entropy.

3 A new polarization lemma for the IID problem

The Zero-Knowledge protocols usually require from the promise problems some parameters that are exponentially close to 0 or 1. Polarizations are reductions from promise problems with worse parameters to promise problems that can be solved by the protocol. For example, there is a polarization for the SD problem which transforms $SD^{a,b}$ with $a^2 > b$ to $SD^{1-2^{-k},2^{-k}}$ for any $k \in poly(n)$.

The best polarization that was known for IID was that $IID^{1/n^2,1-1/n^2}$ reduces to $IID^{2^{-k},1-2^{-k}}$ and henceforth $IID^{1/n^2,1-1/n^2}$ is complete for $NISZK_{|h}$ ([BG03]). We will show here that $IID^{a,b}$ is complete for $NISZK_{|h}$ with $b > 2a$ (a and b are constants). We first improve an upper bound on statistical difference and then use it to prove this new polarization lemma for the IID problem. The proofs are presented in Appendix A.

To prove a polarization lemma on the SD problem, the following bounds were used :

Fact 1 ([Vad99])**.** *Let X, Y two probability distributions st. $SD(X,Y) = \delta$. Then*

$$1 - 2\exp^{-k\delta^2/2} \leq SD(X^{\otimes k}, Y^{\otimes k}) \leq k\delta$$

We can improve the upper bound on Statistical Difference to

$$SD(X^{\otimes k}, Y^{\otimes k}) \leq 1 - (1-\delta)^k \leq k\delta$$

by using the following lemma (proof in Appendix A).

Lemma 1. *Let X, Y, Z, T four probability distributions with $SD(X,Y) = \delta_1$ and $SD(Z,T) = \delta_2$. Then,*

$$SD(X \otimes Z, Y \otimes T) \leq 1 - (1-\delta_1)(1-\delta_2) = \delta_1 + \delta_2 - \delta_1\delta_2$$

Using the new upper bound, we prove in Appendix A that

Theorem 1. *$IID^{a,b}$ is $NISZK_{|h}$ complete for any a, b with $b > 2a$ (a, b constants).*

In the next section ,we will use this polarization lemma to show that $NISZK_{|h} = SZK$. This will, in turn, imply that $IID^{a,b}$ is complete for $b^2 > a$ using the polarization used for the SD problem. Our initial polarization is still interesting because it shows that problems like $IID^{1/10,3/10}$ are in SZK, something which was not known before.

4 Equivalence of help and interaction in Statistical Zero-Knowledge

We show here that help and interaction are equivalent in the Statistical Zero-Knowledge setting

Theorem 2. $SZK = NISZK_{|h}$

Proof. We know that $NISZK_{|h} \subseteq SZK$ because IID, the complete problem of $NISZK_{|h}$, trivially reduces to $\overline{SD}$, the complete problem of SZK. In what follows we also prove the opposite inclusion, *i.e.* $SZK \subseteq NISZK_{|h}$ (Lemma 2). $\square$

In [GB00], the authors claimed to have proven this theorem, but due to a flaw they retracted it in [BG03]. Their reduction from the SZK-complete problem ED to IID was in fact only a reduction to $\overline{SD}$. Nevertheless, inspired by their method we show a reduction from $\overline{EA}$ to IID.

In order to prove that help can replace interaction we start by reducing the SZK-complete problem $\overline{ED}$ to several instances of EA and $\overline{EA}$. We know that $EA \in NISZK_{|h}$ (since by definition $NISZK \subseteq NISZK_{|h}$) so it remains to show the following two things:

1. $\overline{EA} \in NISZK_h$: In order to this, we use similar tools to the ones in [Vad99] and especially the "Complementary use of messages" originally used in [Oka96].
2. $NISZK_{|h}$ has some boolean closure properties : this will allow us to reduce $\overline{ED}$ to a single instance of IID.

4.1 $\overline{EA}$ belongs to Non-Interactive Statistical Zero-Knowledge with help

To show that $\overline{EA} \in NISZK_{|h}$, we reduce the $\overline{EA}$ problem to the IID problem which is complete for $NISZK_{|h}$.

Let X an instance of $\overline{EA}^t$, *i.e.* an instance of $\overline{EA}$ with approximation parameter t. Let $k = poly(m)$, where m is the input size and define $X' = X^{\otimes s}$ with $s = 4km^2$. Note that the input size of X' is $m' = sm$ and $H(X') = sH(X)$. We have

Claim 1. *Let $Z = X' \otimes I$, where I is the uniform distribution. We can create Z' in polynomial time such that :*

- $X \in \overline{EA}^t_Y \Rightarrow SD(Z, Z') \leq 2^{-\Omega(k)}$
- $X \in \overline{EA}^t_N \Rightarrow Disj(Z, Z') \geq 1 - 2^{-\Omega(k)}$

Proof. Construct Z' as following:

Z' : choose $r \in_R \{0,1\}^{m'}$, $x = X'(r)$, $h \in_R \mathcal{H}_{m'+st,m'}$, $u \in_R \{0,1\}^{st}$. return $(x, (h, h(r,u)))$.

Note that Z' is of the form $Z' = X' \otimes A$ so we need to show that, when fixing $x \in X'$, we have either $SD(I, A)$ small (in the Yes instance) or $Disj(I, A)$ large (in the No instance). From the Flattening lemma (see Preliminaries) we have

Fact 2.

1. *X' is Δ-flat with $\Delta = 2\sqrt{k}m^2$. s was chosen such that $s = 2\sqrt{k}\Delta$.*
2. *Let $x \leftarrow X'$. $Pr[x$ is $\sqrt{k}\Delta$-typical$] \geq 1 - 2^{-\Omega(k)}$.*

For $x \in X'$, let $wt(x) = \log |\{r \mid X'(r) = x\}|$. When $x \in X'$ is fixed, the number of different possible inputs (r, u) that are hashed is $2^{wt(x)+st}$. From the flattening lemmas, it is easy to see that if $H(X) \leq t - 1$ then $wt(x)$ will be large with high probability whereas if $H(X) \geq t + 1$ then $wt(x)$ will be small with high probability. In more detail,

(i) $\mathbf{H(X) \leq t - 1}$.

For all $x \in X'$ which are $\sqrt{k}\Delta$-typical we have $\left|\log \frac{1}{2^{m'}}|\{r \mid X'(r) = x\}| + H(X')\right| \leq \sqrt{k}\Delta$. Hence,

$$wt(x) \geq m' - sH(X) - \sqrt{k}\Delta \geq m' - st + s - \sqrt{k}\Delta \geq m' - st + \sqrt{k}\Delta.$$

Therefore, the number of inputs (r, u) such that $X'(r) = x$ and $u \in \{0,1\}^{st}$ is greater than $2^{m'+\sqrt{k}\Delta} \geq 2^{m'+k}$. By the leftover hash lemma (see Preliminaries), $SD((h, h(r,u)), I) \leq O(2^{-\Omega(k)})$. By Fact 2, the probability of a $\sqrt{k}\Delta$-typical x is larger than $\geq 1 - 2^{-\Omega(k)}$ and hence we can conclude that $SD(Z, Z') \leq 2^{-\Omega(k)}$.

(ii) $\mathbf{H(X) \geq t + 1}$.

For all $x \in X'$ which are $\sqrt{k}\Delta$-typical we have

$$wt(x) \leq m' - sH(X) + \sqrt{k}\Delta \leq m' - st - s + \sqrt{k}\Delta \leq m' - st - \sqrt{k}\Delta.$$

Therefore, the number of inputs (r, u) such that $X'(r) = x$ and $u \in \{0,1\}^{st}$ is smaller than $2^{m'-\sqrt{k}\Delta} \leq 2^{m'-k}$. Since we hash at most $2^{m'-k}$ values into $\{0,1\}^{m'}$, we get only a 2^{-k} fraction of the total support and hence $Disj(I, h(r,u)) \geq 1 - 2^{-\Omega(k)}$. By Fact 2, the probability of a $\sqrt{k}\Delta$-typical x is larger than $\geq 1 - 2^{-\Omega(k)}$ and hence we can conclude that $Disj(Z, Z') \geq 1 - 2^{-\Omega(k)}$.

□

From the distribution X, we have created Z, Z' in polynomial time such that :

- $X \in \overline{EA}_Y \Rightarrow (Z, Z') \in IID_Y$.
- $X \in \overline{EA}_N \Rightarrow (Z, Z') \in IID_N$.

So $\overline{EA} \preccurlyeq IID$ and from the completeness of IID for $NISZK_{|h}$, we have $\overline{EA} \in NISZK_{|h}$.

4.2 Closure properties for $NISZK_{|h}$

Closure properties have been widely used in the study of Zero-Knowledge classes (see [DDPY94] or [SV98]). Every promise problem $\Pi \in NISZK_{|h}$ reduces to the IID promise problem and hence, we just have to concentrate on this problem. Note that this problem is very similar to the $\overline{SD}$ promise problem and hence we use similar techniques to those used to show closure properties for SZK from the SD problem. In our case, we just need to show some limited closure properties that will be enough to prove that $\overline{ED} \in NISZK_{|h}$.

Definition 7. *Let $\Pi^1, \ldots, \Pi^k$ some promise problems. We define $AND(\Pi^1, \ldots, \Pi^k)$:*

- $(X^1, \ldots, X^k) \in AND(\Pi^1, \ldots, \Pi^k)_Y \Rightarrow \forall i \in \{1, \ldots, k\}\ X^i \in \Pi^i_Y$
- $(X^1, \ldots, X^k) \in AND(\Pi^1, \ldots, \Pi^k)_N \Rightarrow \exists i \in \{1, \ldots, k\}\ X^i \in \Pi^i_N$

In the AND definition, we assume k to be of size polynomial in the input size, i.e. $k \in poly(n)$.

Definition 8. *Let Π, Ω two promise problems. We define $OR(\Pi, \Omega)$:*

- $(X,Y) \in OR(\Pi,\Omega)_Y \Rightarrow X \in \Pi_Y$ *or* $Y \in \Omega_Y$
- $(X,Y) \in OR(\Pi,\Omega)_N \Rightarrow X \in \Pi_N$ *and* $Y \in \Omega_N$

We will show that $NISZK_{|h}$ is closed under AND and OR which is enough for our purposes.

Claim 2. *$NISZK_{|h}$ is closed under AND.*

Proof. Let $\Pi^1,\dots,\Pi^k$ in $NISZK_{|h}$ and $(A^1,\dots,A^k)$ an instance of $AND(\Pi^1,\dots,\Pi^k)$. We reduce each Π^i to the IID problem which means that we transform each A^i into a pair of distributions (X^i,Y^i) such that $A^i \in \Pi^i_Y \Rightarrow (X^i,Y^i) \in IID_Y$ and $A^i \in \Pi^i_N \Rightarrow (X^i,Y^i) \in IID_N$. Let $X = X^1 \otimes \dots \otimes X^k$ and $Y = Y^1 \otimes \dots \otimes Y^k$. We first polarize each pair (X^i,Y^i) such that $(X^i,Y^i) \in IID^{1/n^2k,1-1/n^2}$ (which is possible since $k \in poly(n)$). Then, we use the following fact from [Vad99] and [BG03]:

Fact 3.
- $SD(X,Y) \leq \sum_i SD(X^i,Y^i)$
- $Disj(X,Y) \geq \max_i Disj(X^i,Y^i)$

From this fact, we can easily see that $(A^1,\dots,A^k) \in AND(\Pi^1,\dots,\Pi^k)_Y \Rightarrow (X,Y) \in IID_Y$ and that $(A^1,\dots,A^k) \in AND(\Pi^1,\dots,\Pi^k)_N \Rightarrow (X,Y) \in IID_N$, which concludes our proof. □

Claim 3. *$NISZK_{|h}$ is closed under OR.*

Proof. Let $\Pi,\Omega \in NISZK_{|h}$. Let I an instance of Π and J an instance of Ω. We reduce I to a pair of distributions (X'_0,Y'_0) such that $I \in \Pi_Y \Rightarrow (X'_0,Y'_0) \in IID_Y$ and $I \in \Pi_N \Rightarrow (X'_0,Y'_0) \in IID_N$. Similarly, we reduce J to a pair of distributions (X'_1,Y'_1). By using fact 7 from Appendix A, we create (X_0,Y_0) and (X_1,Y_1) that are instances of mut-$IID^{1/n^2,\frac{1}{2}(1-1/n^2)} \preccurlyeq$ mut-$IID^{1/20,1/3}$ (for sufficiently big n). Now, consider the following two distributions

A : pick $b \in_R \{0,1\}$, return a sample of $X_b \otimes Y_b$.
B : pick $b \in_R \{0,1\}$, return a sample of $X_b \otimes Y_{\bar{b}}$.

This is a generalization of the XOR transformation and was used in [Vad99] to show closure properties for SZK. We now use the following fact

Fact 4. *[Vad99] and [BG03]*
- $SD(A,B) = SD(X_0,Y_0) * SD(X_1,Y_1)$
- *mut-$Disj$*$(A,B) =$ *mut-$Disj$*$(X_0,Y_0) *$ *mut-$Disj$*(X_1,Y_1)

From this, we can easily see that $(X_0,Y_0) \in$ mut-$IID_Y^{1/20,1/3}$ or $(X_1,Y_1) \in$ mut-$IID_Y^{1/20,1/3} \Rightarrow (A,B) \in IID_Y^{1/20,1/9}$. Similarly, if $(X_0,Y_0) \in$ mut-$IID_N^{1/20,1/3}$ and $(X_1,Y_1) \in$ mut-$IID_N^{1/20,1/3} \Rightarrow (A,B) \in$ mut-$IID_N^{1/20,1/9}$. We have therefore reduced $OR(\Pi,\Omega)$ to a single instance of mut-$IID^{1/20,1/9}$. Since mut-$IID^{1/20,1/9} \preccurlyeq IID^{1/20,1/9}$ and by our new polarization lemma, $IID^{1/20,1/9} \in NISZK_{|h}$ we conclude that $OR(\Pi,\Omega) \in NISZK_{|h}$. □

4.3 Help can replace interaction

We can now prove that help can replace interaction and hence conclude the proof of Theorem 2.

Lemma 2. $SZK \subseteq NISZK_{|h}$

Proof. We show that $\overline{ED} \in NISZK_h$, which will allow us to conclude since $\overline{ED}$ is complete for SZK. Let (X, Y) an instance of $\overline{ED}$.

Fact 5 ([Vad99]). *Let $X' = X^{\otimes 3}$ and $Y' = Y^{\otimes 3}$. Let n the output size of X' and Y'. It holds that :*

$$
\begin{aligned}
(X,Y) \in \overline{ED}_Y &\Leftrightarrow \forall t \in \{1,\ldots,n\} \left[(X' \in \overline{EA}^t_Y) \vee (Y' \in EA^t_Y)\right] \\
(X,Y) \in \overline{ED}_N &\Leftrightarrow \exists t \in \{1,\ldots,n\} \left[(X' \in \overline{EA}^t_N) \wedge (Y' \in EA^t_N)\right]
\end{aligned}
$$

This fact comes from the following observation: if $(X, Y) \in \overline{ED}_N$ then $H(X') \geq H(Y') + 3$ and hence, there exists $t \in [n]$ such that $H(X') \geq t + 1$ and $H(Y') \leq t - 1$. On the other hand, if $H(Y') \geq H(X') + 3$ then $\forall t,\ H(X') \leq t - 1$ or $H(Y') \geq t + 1$.

We have already shown that EA and $\overline{EA}$ are in $NISZK_{|h}$. Moreover, we have closure under OR, and hence for all t there exists a promise problem $\Pi^t \in NISZK_{|h}$ and an input A^t such that

$$
\begin{aligned}
(X',Y') \in OR(\overline{EA}^t, EA^t)_Y &\Rightarrow A^t \in \Pi^t_Y \\
(X',Y') \in OR(\overline{EA}^t, EA^t)_N &\Rightarrow A^t \in \Pi^t_N
\end{aligned}
$$

Therefore,

$$
\begin{aligned}
(X,Y) \in \overline{ED}_Y &\Rightarrow \forall t \in \{1,\ldots,n\} A^t \in \Pi^t_Y \\
(X,Y) \in \overline{ED}_N &\Rightarrow \exists t \in \{1,\ldots,n\}\ A^t \in \Pi^t_N
\end{aligned}
$$

and from the closure under AND we conclude that $\overline{ED} \in NISZK_{|h}$. □

This theorem has some interesting corollaries.

Corollary 1. *$NISZK_{|h}$ has all the properties of SZK like closure under complement or closure under boolean formula.*

It is interesting to find a non-interactive class that has all the properties of SZK. It means that the power of SZK lies only in the fact that there is a trusted access to the distributions (from the Verifier or from the Dealer).

Corollary 2. *The IID problem is complete for SZK.*

We have here a new complete problem for SZK. This problem is easier to manipulate and could be used to find other results about SZK.

5 Complete problems for $QNISZK$

In this section we study complete problems for the class $QNISZK$. Note that Kobayashi showed a complete problem for the case of Non-Interactive Perfect Zero-Knowledge, however was unable to extend his proof to the case of Statistical Zero-Knowledge.

We continue this line of work and give two complete problems for $QNISZK$, the *Quantum Entropy Approximation* and the *Quantum Statistical Closeness to Uniform.* These are the natural generalizations of the $NISZK$-complete problems EA, SCU. Ben-Aroya and Ta-Shma showed that QEA reduced to QSD. In fact, during their proof, they showed that $QEA \in QSCU^{a,b}$ but these parameters a, b were not good enough to show that $QEA \in QNISZK$. We will modify their proof to show that $QEA \in QNISZK$ and then conclude using similar techniques than the ones used in the classical case (see [GSV99] as well as the analysis of $QNISZK$ done by Kobayashi [Kob03]). The proof will follow from the following three lemmas.

Lemma 3. *$QEA \in QNISZK$.*

Proof. We modify the proof of [BT07] to show that $QEA \in QNISZK$. Let X an instance of QEA^t with input size m and $\mathbb{I}$ the totally mixed state.

Claim 4 ([BT07])**.** *We can create X' such that*

- $X \in QEA_Y \Rightarrow SD(X', \mathbb{I}) \leq 5\epsilon$
- $X \in QEA_N \Rightarrow SD(X', \mathbb{I}) \geq \frac{1}{2qm}$

where $q \geq 2\log(1/\epsilon) + \log(qm) + O(1)$ *and also* $q \geq \sqrt{\log(1/\epsilon)}\sqrt{q}n + 1$.

We apply this claim with the following parameters : fix $\epsilon = 2^{-k}$ with $k \in poly(n)$ and then $q \in poly(n)$ that satisfies the constraints. Let X' be the resulting distribution. Now let $r = 8k(qm)^2 \in poly(n)$ and $Y = X'^{\otimes r}$. By using bounds on Statistical Difference, we have

- $X \in QEA_Y \Rightarrow SD(X', \mathbb{I}) \leq 5r\epsilon \leq 2^{-\Omega(k)}$
- $X \in QEA_N \Rightarrow SD(X', \mathbb{I}) \geq 1 - 2^{-k}$

Kobayashi showed in [Kob03] that $QSCU^{2^{-k}, 1-2^{-k}} \in QNISZK$ and hence by our claim that $QEA \preccurlyeq QSCU^{2^{-k}, 1-2^{-k}}$ we conclude that $QEA \in QNISZK$. □

Lemma 4. *$QSCU \preccurlyeq QEA$.*

Proof. We use the following fact about the relation of trace distance and von Neumann entropy

Fact 6. *Let X a quantum state of dimension n.*

1. $\|X - \mathbb{I}\|_{tr} \leq \alpha \Rightarrow S(X) \geq n(1 - \alpha - 1/2^n)$.
2. $\|X - \mathbb{I}\|_{tr} \geq \beta \Rightarrow S(X) \leq n - \log(\frac{1}{1-\beta})$.

Let X a quantum mixed state of dimension $n \geq 16$. $\|X - \mathbb{I}\|_{tr} \leq 1/n \Rightarrow S(X) \geq n - 2$. $\|X - \mathbb{I}\|_{tr} \geq 1 - 1/n \Rightarrow S(X) \leq n - 4$. When $n \leq 16$, we can solve $QSCU$ polynomially. We have a reduction from $QSCU$ to QEA. □

Lemma 5. *Every problem in $QNISZK$ reduces to $QSCU$.*

Proof. The proof of hardness for $QNIPZK$ extends naturally to this problem. We will not repeat the proof here. The interested reader can see [Kob03] for this proof. □

It now follows immediately that

Theorem 3. *QEA and $QSCU$ are complete for $QNISZK$.*

Proof. $QSCU$ is hard for $QNISZK$ and $QSCU \preccurlyeq QEA$ so both problems are hard for $QNISZK$. $QEA \in QNISZK$ and $QSCU \preccurlyeq QEA$ so they are both in $QNISZK$. □

6 Help in quantum Non-Interactive Zero-Knowledge protocols

In classical Non-Interactive Zero-Knowledge, the Prover and Verifier start with a shared uniformly random string, which is independent of their input. Classical help was a natural generalization of this and was defined as a shared string created by a trusted third party with polynomial power (the Dealer) who has access to the input.

In quantum Non-Interactive Zero-Knowledge, the Prover and Verifier share a maximally entangled state $\sum_i |i\rangle|i\rangle$, with the Prover having the first register and the Verifier the second. Note that this state is pure and independent of the input x.

Help with unitaries We define quantum help as a generalization of the maximally entangled state. We suppose here that there is a trusted Dealer with quantum polynomial power that performs a unitary U_x and creates a state h_{PV} in the space $\mathcal{P} \times \mathcal{V}$. The Prover gets $h_P = Tr_{\mathcal{V}}(h_{PV})$ and the Verifier gets $h_V = Tr_{\mathcal{P}}(h_{PV})$. Note that the state h_{PV} is a pure state and depends on the input.

Definition 9. *We say that $\Pi \in QNISZK_{|h}$ if there is a non-interactive protocol $\langle D, P, V\rangle$ that solves Π with the Zero-Knowledge property, where the Verifier and the Prover share a pure state h_{PV} created by a Dealer D that has quantum polynomial power and access to the input. They also start with qubits initialized at $|0\rangle$. We denote by $\langle D, P, V\rangle$ the entire protocol.*

Next, we prove that help and interaction are equivalent in the quantum setting, but with a much easier proof than in the classical case.

Theorem 4. $QNISZK_{|h} = QSZK$

Proof. We start by showing that $QNISZK_{|h} \subseteq QSZK$. Let $\Pi \in QNISZK_{|h}$ and $\langle D, P, V\rangle$ denote the protocol. Since h_{PV} is a pure state, we can create another protocol $\langle \widetilde{P}, \widetilde{V}\rangle$ where the Verifier takes the place of the Dealer. Because the Dealer is a unitary (and has no private qubits), this can be done. The protocol is the same so soundness and completeness are preserved. The first message in $\langle \widetilde{P}, \widetilde{V}\rangle$ can be simulated because the circuit of the Dealer is public and computable in quantum polynomial time. The second message in $\langle \widetilde{P}, \widetilde{V}\rangle$ can be simulated because of the Zero-Knowledge property of the protocol $\langle P, V\rangle$.

The inclusion $QSZK \subseteq QNISZK_{|h}$ is immediate, since there exists a two message protocol for a $QSZK$-complete problem (see [Wat02]). The first message of the Verifier can be simulated by the Dealer's help. □

Using non-unitaries The unitary restriction is natural when dealing with quantum Zero-Knowledge classes. However, unitary help does not allow the dealer to keep some information private. In fact, we can imagine a stronger quantum help, where the Dealer can perform any quantum operation in order to create the help. For example, he can create a quantum state, keep part of it to himself and share the rest of the state between the Prover and the Verifier.

It is not hard to see, that in this way, the dealer can create an even stronger type of classical help, namely where he can give secret correlated messages to the Verifier and the Prover. Since we know that $NISZK^{SEC} = AM$ (see [PS05]) we can conclude that non-unitary help is very strong. Note also that with non-unitaries we don't know if help and interaction are equivalent. The case of Quantum Zero Knowledge protocols with non-unitary players is indeed very interesting and we refer the reader to [CK07] for more results.

6.1 Quantum Non-Interactive Zero-Knowledge with classical help

We now define two "hybrid" classes, where the Prover and Verifier are quantum, however in the beginning of the protocol they only share classical information. These classes have very interesting connections to the class of languages that possess classical zero-knowledge protocols secure against quantum adversaries, *i.e.* the class studied by Watrous [Wat06] and Hallgren *et al* [HKSZ07]. We start by providing some appropriate definitions.

Definition 10. *We say that a circuit C is ϵ-probabilistic if*

$$\forall x,\ \exists! y,\ Pr(C(x) = y) \geq 1 - \epsilon$$

This y will be called the natural image of x and will be noted $Nat_C(x)$

We now define q-samplable distributions as follows:

Definition 11. *A distribution $D \in \mathcal{P}$ is called q-samplable if it can be represented by a 2^{-k}-probabilistic circuit C ($k \in poly(n)$) with classical input and output and such that in order to compute $C(x)$ for any x, we need a BQP machine.*

To deal with q-samplable distributions, we also extend the definition of Disjointness to probabilistic circuits.

Definition 12.

$$Disj(X, Y) = \frac{1}{2^n} \sum_{r \in \{0,1\}^n} \max_y (Pr(Y(y) = X(r)))$$

$Disj(X, Y)$ must be understood as follows : "If I take a random x of X, and I'm given a y (potentially the best), what is the probability that $Y(y) = x$?"

Note that when the second distribution (Y) is described by a deterministic circuit then this notion of disjointness is equivalent to the original one.

From this fact, we will show a simple relationship between Statistical Difference and Disjointness. In the case of deterministic distributions, we know that $Disj(X, Y) \leq SD(X, Y)$.

Lemma 6. *Let (X, Y) be 2 ϵ-probabilistic circuits. We have : $Disj(X, Y) \leq SD(X, Y) + 2\epsilon$.*

Proof. Let (X, Y) be 2 ϵ-probabilistic circuits. We define $\widetilde{Y}$ as following : $\widetilde{Y}(r) = Nat_Y(r)$. We can easily see that $SD(\widetilde{Y}, Y) \leq \epsilon$ and that $Disj(X, Y) \leq Disj(X, \widetilde{Y}) + \epsilon$. From this, we conclude that :

$$Disj(X, Y) \leq Disj(X, \widetilde{Y}) + \epsilon \leq SD(X, \widetilde{Y}) + \epsilon \leq SD(X, Y) + 2\epsilon$$

□

Note that 2^{-n}-probabilistic circuits behave similarly (with exponentially small difference) to deterministic circuits. This means that we can apply polarization lemmas and extend all the completeness theorems that were shown with classical distributions to q-samplable distributions. We can now study $QNISZK_{|ch}$.

Definition 13. *We say that $\Pi \in QNISZK_{|ch}$ if there exists a non-interactive protocol $\langle P, V \rangle$ that solves Π with the Zero-Knowledge property where the Verifier and the Prover start with some classical help h distributed over a distribution D prepared by a trusted Dealer with quantum polynomial power. We want the dealer D and the simulation S to be q-samplable distributions. The prover and the verifier also start with $|0\rangle$ qubits. We denote $\langle D, P, V \rangle$ the entire protocol.*

Let us define the problem IID^q: Let X, Y two q-samplable probability distributions which are describes by 2^{-n}-probabilistic circuits

- $(X, Y) \in IID^q_Y \Rightarrow SD(X, Y) \leq 1/4$
- $(X, Y) \in IID^q_N \Rightarrow Disj(X, Y) \geq 3/4$

We prove that this problem is complete for $QNISZK_{|ch}$ by the following two lemmas.

Lemma 7. $IID^q \in QNISZK_{|ch}$.

Proof. Let (X, Y) an instance of IID^q. Using our polarization lemma, we construct (X', Y') such that $(X, Y) \in IID^q_Y \Rightarrow SD(X', Y') \leq 2^{-k}$ and $(X, Y) \in IID^q_N \Rightarrow Disj(X', Y') \geq 1 - 2^{-k}$ for some $k \in poly(n)$. We use the same protocol as for the classical case:

Protocol in $QNISZK_{|ch}$ for the IID^q problem

H : create $x' \leftarrow X'$ and reveal it.

P : send r such that $Y'(r) = x'$.

V : Verify that $Y'(r) = x'$

This protocol is the same as the one used in [BG03]. Note that the completeness and soundness correspond exactly to the Disjointness of the two distributions and hence they follow from Lemma 6. Moreover, working on q-samplable distributions doesn't change the Zero-Knowledge property and hence it follows immedaitely from [BG03]. ☐

Lemma 8. *Every problem in $QNISZK_{|ch}$ reduces to IID^q*

Proof. The proof of Ben-Or and Gutfreund that IID is hard for $NISZK_{|h}$ can be naturally extended to the case where the Verifier and the Dealer are BQP machines by taking into account that the distributions are now q-samplable.

Consider a promise problem $\Pi \in QNISZK_{|ch}$. Let $\langle D, P, V \rangle$ be a non-interactive protocol for Π with completeness $c(k)$, soundness $s(k)$and simulator deviation $\mu(k)$ with $1 - c(k), s(k), \mu(k) \in negl(k)$. Let x an instance of Π. Consider now the two following distributions :

D_0 : run the Dealer D on x.

D_1 : run the simulator $k \in poly(n)$ times on x with the same coins to get k samples (h, m_P). Note that these copies are the same with exponentially high probability because the simulator is $2^{-O(k)}$-probabilistic. Run the accepting procedure A on each copy of (x, h, m_P). Output h if V accepts the majority of the times and $\perp$ otherwise.

- If $x \in \Pi_Y$ then the Verifier will accept the majority of times with probability $(1 - 2^{-O(k)})$ because of completeness. In this case, the distribution D_1 is equal to the simulation of the help, which has statistical difference $\mu(k)$ from the real help. Since the distribution D_0 is the distribution of the real help, we have $SD(D_0, D_1) \leq \mu(k) + 2^{-O(k)} \leq 1/4$ and $(D_0, D_1) \in IID^q_Y$.
- Let $x \in \Pi_N$ and B be the set of help strings, such that $h \in B \Rightarrow \exists\ m_P\ Pr[A(x, h, m_P) = Yes] \geq 1/3$ where A is the verifying procedure of V. The probability that D_0 produces a sample $h \in B$ (and therefore a sample in $B \cup \{\perp\}$) is $\leq 3s(k)$ due to the soundness condition. It also holds that the probability that D_1 produces a sample in $B \cup \{\perp\}$ is $\geq 1 - O(2^{-k})$. This can seen as follows: the probability that D_1 outputs $h \in \overline{B}$ is equal to the probability that the Verifier accepts the majority of times, when running A k times with $h \in \overline{B}$, which happens with probability at most $2^{-O(k)}$. We conclude that $Disj(D_0, D_1) \geq (1 - 2^{(O(k))})(1 - 3s(k)) \geq 3/4$ and $(D_0, D_1) \in IID^q_N$

Since the Dealer and Simulator are q-samplable, the distributions D_0 and D_1 are also q-samplable. □

and hence D_1 is $2^{-O(k)}$-probabilistic

From Lemma 7 and Lemma 8, we have

Theorem 5. *IID^q is complete for $QNISZK_{|ch}$.*

Similarly, we can define Quantum Non-Interactive Zero-Knowledge where the Prover and the Verifier share a classical random string. We denote this class $QNISZK_r$. Let us define SCU^q as the statistical closeness to uniform applied on a q-samplable distribution. By the same arguments SCU^q is complete for $QNISZK_{|r}$.

Using these complete problems, we have the following interesting corollary

Corollary 3. *In $QNISZK_{|r}$ and $QNISZK_{|ch}$, the Prover sends a classical message.*

Proof. This is true because there is a protocol for IID^q and SCU^q where the Prover sends a classical message and these two problems are complete. □

Now denote by SZK_q the class SZK where the Verifier and simulation use quantum polynomial power. In other words, this is the class of languages that have classical protocols which are Zero-Knowledge against quantum Verifiers. Similarly, define the classes $HVSZK_q$ and $NISZK_{|h,q}$ (where both the Verifier and the Dealer use quantum power). The class SZK_q was studied by Watrous ([Wat06]) and Hallgren *et al* [HKSZ07]. It remains open to show whether these three classes are equal to each other, which is true when the Verifier is classical.

Note that by corollary 3, we have that $QNISZK_{|ch} = NISZK_{|h,q}$. Using our analysis of $NISZK_{|h}$, we can show the following :

Theorem 6. $NISZK_{|h,q} = HVSZK_q$

Proof. Similar to the case of $HVSZK$, we can show that SD^q is complete for $HVSZK_q$ (see also [Vad99]) where SD^q is the natural extension of SD applied to q-samplable distributions. From section 4, we know a reduction from SD to IID. The same reduction works from SD^q to IID^q so $HVSZK_q \subset QNISZK_{|ch} = NISZK_{|h,q}$. Because IID^q trivially reduces to SD^q, we have $HVSZK_q = NISZK_{|h,q}$. $\square$

7 Conclusion and further work

Our work settles the question of the role of help in Zero-Knowledge protocols by showing that it is equivalent to interaction. In other words, we showed that the only thing that is important to create a statistical Zero-Knowledge proof is a trusted access to the input (from the Dealer or from the honest Verifier). This will hopefully shed some light into the relation of Non-Interactive and Interactive Zero-Knowledge, which still remains open.

In the quantum setting, we gave the first formal definition of help for Zero-Knowledge protocols. We showed that quantum help is also equivalent to interaction and that the case of classical help is closely related to the class of languages that have classical zero-knowledge protocols secure against quantum Verifiers. It would be interesting to see if quantum help could also give some interesting results concerning the class SZK_q, and especially whether $SZK_q = HVSZK_q$.

References

[BG03] Michael Ben-Or and Danny Gutfreund. Trading help for interaction in statistical zero-knowledge proofs. *J. Cryptology*, 16(2):95–116, 2003.

[BT07] Avraham Ben-Aroya and Amnon Ta-Shma. Quantum expanders and the quantum entropy difference problem. *ArXiv Quantum Physics e-prints*, quant-ph/0702129, 2007.

[CK07] André Chailloux and Iordanis Kerenidis. Using non-untiaries in quantum zero-knowledge protocols. *Manuscript*, 2007.

[DDPY94] Alfredo De Santis, Giovanni De Crescenzo, Giuseppe Persiano, and Moti Yung. On monotone formula closure of SZK. In *Proc. 26th ACM Symp. on Theory of Computing*, pages 454–465, Montreal, Canada, 1994. ACM.

[DMP88] Alfredo De Santis, Silvio Micali, and Giuseppe Persiano. Non-interactive zero-knowledge proof systems. In *CRYPTO '87: A Conference on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology*, pages 52–72, London, UK, 1988. Springer-Verlag.

[GB00] Danny Gutfreund and Michael Ben-Or. Increasing the power of the dealer in non-interactive zero-knowledge proof systems. In *ASIACRYPT*, pages 429–442, 2000.

[GMR89] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. *SIAM J. Comput.*, 18(1):186–208, 1989.

[GMW91] Oded Goldreich, Silvio Micali, and Avi Wigderson. Proofs that yield nothing but their validity or all languages in np have zero-knowledge proof systems. *J. ACM*, 38(3):690–728, 1991.

[GSV99] Oded Goldreich, Amit Sahai, and Salil Vadhan. Can statistical zero knowledge be made noninteractive? or on the relationship of SZK and NISZK. *Lecture Notes in Computer Science*, 1666:467–484, 1999.

[HKSZ07] Sean Hallgren, Alexandra Kolla, Pranab Sen, and Shengyu Zhang. All problems in statistical zero-knowledge have a classical protocol secure against quantum verifiers. *Manuscript*, 2007.

[Kob03] Hirotada Kobayashi. Non-interactive quantum perfect and statistical zero-knowledge. volume 2906, pages 178–188, 2003.

[Kob07] Hirotada Kobayashi. General Properties of Quantum Zero-Knowledge Proofs. *ArXiv Quantum Physics e-prints*, quant-ph/0705.1129, May 2007.

[Oka96] Tatsuaki Okamoto. On relationships between statistical zero-knowledge proofs. In *STOC '96: Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 649–658, New York, NY, USA, 1996. ACM Press.

[PS05] Rafael Pass and Abhi Shelat. Unconditional characterizations of non-interactive zero-knowledge. In *CRYPTO '05*, pages 118–134, 2005.

[SV98] Amit Sahai and Salil Vadhan. *Manipulating statistical difference.* In Panos Pardalos, Sanguthevar Rajaseekaran, and Jose Rolim, editors, Proceedings of the DIMACSWorkshop on RandomizationMethods in Algorithm Design, Princeton, NJ, 1998. American Mathematical Society, 1998.

[Vad99] Salil Pravin Vadhan. *A study of statistical zero-knowledge proofs.* PhD thesis, 1999. Supervisor-Shafi Goldwasser.

[Wat02] John Watrous. Limits on the power of quantum statistical zero-knowledge. In *FOCS '02: Proceedings of the 43rd Symposium on Foundations of Computer Science*, pages 459–468, Washington, DC, USA, 2002. IEEE Computer Society.

[Wat06] John Watrous. Zero-knowledge against quantum attacks. In *STOC '06: Proceedings of the thirty-eighth annual ACM Symposium on Theory of Computing*, pages 296–305, New York, NY, USA, 2006. ACM Press.

A Details of the polarization of IID

Proof. (Lemma 1) Define $w_S(X) = \sum_{i \in S} x_i$ to be the weight of $X \in P_n$ on the set $S \subseteq \{0,1\}^n$, $S(X,Y) = \{i \in \{0,1\}^n | \ x_i \leq y_i\}$ and $\overline{S}(X,Y)$ the complement. Fix X, Y, Z, T four probability distributions with $c_1 = 1 - \delta_1 = SC(X,Y)$, $c_2 = 1 - \delta_2 = SC(Z,T)$ and $c = 1 - \delta = SC(X \otimes Z, Y \otimes T)$. Let $A = S(X,Y)$, $A' = S(Z,T)$, $\overline{A}$ and $\overline{A'}$ the complementary sets, $\alpha_1 = w_A(X)$, $\beta_1 = w_A(Y)$, $\alpha_2 = w_{A'}(Z)$ and $\beta_2 = w_{A'}(T)$. We have :

$$c_1 = \sum_i \min(x_i, y_i) = w_A(X) + w_{\overline{A'}}(Y) = \alpha_1 + 1 - \beta_1 \qquad \text{and} \qquad c_2 = \alpha_2 + 1 - \beta_2$$

We now show that $c \geq c_1 c_2$.

$$\begin{aligned}
c &= \sum_{i,j} \min(x_i z_j, y_i t_j) \\
&= \sum_{i \in A, j \in A'} \min(x_i z_j, y_i t_j) + \sum_{i \in A, j \in \overline{A'}} \min(x_i z_j, y_i t_j) \\
&\quad + \sum_{i \in \overline{A}, j \in A'} \min(x_i z_j, y_i t_j) + \sum_{i \in \overline{A}, j \in \overline{A'}} \min(x_i z_j, y_i t_j) \\
&\geq \sum_{i \in A j \in A'} x_i z_j + \sum_{i \in A j \in \overline{A'}} x_i t_j + \sum_{i \in \overline{A} j \in A'} y_i z_j + \sum_{i \in \overline{A} j \in \overline{A'}} y_i t_j \\
&\geq \alpha_1 \alpha_2 + \alpha_1 (1 - \beta_2) + \alpha_2 (1 - \beta_1) + (1 - \beta_1)(1 - \beta_2) \\
&\geq c_1 c_2
\end{aligned}$$

By replacing the statistical closeness by the statistical difference, we get

$$\delta \leq 1 - (1 - \delta_1)(1 - \delta_2)$$

□

Proof. (Theorem 1) Let two constants a, b' such that $1 > b' > 2a > 0$. First note that $IID^{a,b'}$ is hard for $NISZK_{|h}$ by making a reduction from $IID^{1/n^2, 1-1/n^2}$ and hence, we just need to reduce $IID^{a,b'}$ to $IID^{1/n^2, 1-1/n^2}$. Let $b = b'/2$. We do this reduction in three steps:

1. It holds that $IID^{a,b'} \preccurlyeq$ mut-$IID^{a,b}$. This point was proven in [BG03] and will not be proven here again.
2. We show that mut-$IID^{a,b} \preccurlyeq$ mut-$IID^{\phi - \alpha, \phi + \alpha}$ with $\alpha > 0$ and $\phi = \frac{\sqrt{5} - 1}{2}$.
3. We show that mut-$IID^{\phi - \alpha, \phi + \alpha} \preccurlyeq IID^{1/n^2, 1-1/n^2}$.

As we said, the first reduction was proven in [BG03]. We will just remind here the construction.

Fact 7. *Let $(X_0, X_1) \in IID^{a,b'}$. Construct (A, B) as following :*

A : pick $r \in_R \{0,1\}$ and $b \in_R \{0,1\}$, return $(X_b(r), b)$.
B : pick $r \in_R \{0,1\}$ and $b \in_R \{0,1\}$, return $(X_b(r), \overline{b})$

We have : $(X_0, X_1) \in IID_Y^{a,b'} \Rightarrow (A, B) \in$ mut-$IID_Y^{a,b}$ and $(X_0, X_1) \in IID_N^{a,b'} \Rightarrow (A, B) \in$ mut-$IID_N^{a,b}$

We show the second reduction by the following lemma:

Lemma 9. *Let a, b such that $b > a$. There exists $\alpha > 0$ such that mut -IID$^{a,b} \preccurlyeq$ mut -IID$^{\phi-\alpha,\phi+\alpha}$.*

Proof. Let X, Y two distributions and a, b with $b > a$ such that $SD(X,Y) \leq a$ or mut-$Disj(X,Y) \geq b$. We are going to construct a pair of distributions (A, B) with the property that either $SD(A,B) \leq \phi - \alpha$ or mut-$Disj(A,B) \geq \phi + \alpha$. Let Γ and Γ' such that $\Gamma, \Gamma' \notin Im(X) \cup Im(Y)$. We define the following distribution:

$$A_{\Gamma,u,X}(x) = \text{ With probability } u \text{ return } X(x) \text{ else return } \Gamma.$$

Similarly, we define the distributions $A_{\Gamma,u,Y}(x), A_{\Gamma',u,X}(x)$. We have

- $SD(X,Y) \leq a \implies SD(A_{\Gamma,u,X}, A_{\Gamma,u,Y}) \leq u^2 a + 2u(1-u) = f(u,a)$.
- mut-$Disj(X,Y) \geq b \implies$ mut-$Disj(A_{\Gamma,u,X}, A_{\Gamma,u,Y}) \geq u^2 b + 2u(1-u) = f(u,b)$
- $SD(X,Y) \leq a \implies SD(A_{\Gamma,u,X}, A_{\Gamma',u,Y}) \leq u^2 a + 2u(1-u) + (1-u)^2 = g(u,a)$
- mut-$Disj(X,Y) \geq b \implies$ mut-$Disj(A_{\Gamma,u,X}, A_{\Gamma',u,Y}) \geq u^2 b + 2u(1-u) + (1-u)^2 = g(u,b)$

Let $\delta = (a+b)/2$. If $\delta = \phi$, then the distributions X, Y already have the desired property. If $\delta > \phi$ then from the fact that the function f is continuous, $f(0,\delta) = 0$ and $f(1,\delta) = \delta$, we conclude that there exists a constant $u_0 \in [0,1]$ such that $f(u_0, \delta) = \phi$. The pair of distributions $(A_{\Gamma,u_0,X}, A_{\Gamma,u_0,Y})$ has the desired property

- $SD(X,Y) \leq a \implies SD(A_{\Gamma,u_0,X}, A_{\Gamma,u_0,Y}) \leq u_0^2 a + 2u_0(1-u_0) = \phi - u_0^2 \frac{b-a}{2}$.
- mut-$Disj(X,Y) \geq b \implies$ mut-$Disj(A_{\Gamma,u_0,X}, A_{\Gamma,u_0,Y}) \geq u_0^2 b + 2u_0(1-u_0) = \phi + u_0^2 \frac{b-a}{2}$.

Similarly, for the case $\delta < \phi$ we use the distributions $(A_{\Gamma,u,X}, A_{\Gamma',u,Y})$ and the function g. $\square$

In order to show our third reduction, we need the following claim : Let X and Y two probability distributions. Denote $(U,V) = XOR(X,Y)$ and let $T : P_n \times P_n \to P_{2n} \times P_{2n}$ be the operator $T(X,Y) = (U \otimes U, V \otimes V)$.

Claim 5. *Let $(A,B) = T(X,Y)$*

$$SD(X,Y) \leq \alpha \Rightarrow SD(A,B) \leq 1 - (1-\alpha^2)^2$$

$$mut\text{ -}Disj(X,Y) \geq \beta \Rightarrow mut\text{ -}Disj(A,B) \geq 1 - (1-\beta^2)^2$$

Proof. The proof follows from our new upper bound on SD, the Direct Product Lemma and the XOR Lemma.

$$\begin{aligned}
SD(A,B) &= SD(U \otimes U, V \otimes V) \ \leq\ 1 - (1 - SD(U,V))^2 \ =\ 1 - (1 - (SD(X,Y))^2)^2 \\
&\leq\ 1 - (1-\alpha^2)^2 \\
\text{mut-}Disj(A,B) &=\ 1 - (1 - \text{mut-}Disj(U,V))^2 =\ 1 - (1 - (\text{mut-}Disj(X,Y))^2)^2 \\
&\geq\ 1 - (1-\beta^2)^2
\end{aligned}$$

$\square$

We now have:

Lemma 10. *Let* $\phi = \frac{\sqrt{5}-1}{2}$. *For any* $\alpha > 0$ *(constant), mut-*$IID^{\phi-\alpha,\phi+\alpha} \preccurlyeq IID^{1/n^2,1-1/n^2}$.

Proof. Let $f(x) = 1 - (1-x^2)^2$ and $U_{i+1} = f(U_i)$. The fixed point of f is $\phi = \frac{\sqrt{5}-1}{2}$. By a straightforward study of f, we can see that if $U_0 \leq \phi - \alpha$ then $U_k \leq 1/n^2$ and if $U_0 \geq \phi + \alpha$ then $U_k \geq 1 - 1/n^2$ with $k = poly(n)$.

Let $(A^i, B^i) = T^i(X, Y)$. By the previous Claim, we know that $SD(A^i, B^i)$ and mut -$Disj(A^i, B^i)$ behave like U_i. Then, for $(A, B) = T^k(X, Y)$ we know that the size of the final distribution is $n \cdot 2^u = poly(n)$ and

$$\begin{aligned} SD(X,Y) \leq \phi - \alpha \quad &\Rightarrow \quad SD(A,B) \leq 1/n^2 \\ \text{mut-}Disj(X,Y) \geq \phi + \alpha \quad &\Rightarrow \quad \text{mut-}Disj(A,B) \geq 1 - 1/n^2 \\ &\Rightarrow \quad Disj(A,B) \geq 1 - 1/n^2 \end{aligned}$$

This concludes the proof. □

Putting these three reductions together we have that for $1 > b' > 2a > 0$:

$$IID^{a,b'} \preccurlyeq \text{mut -}IID^{a,b} \preccurlyeq \text{mut -}IID^{\phi-\alpha,\phi+\alpha} \preccurlyeq IID^{1/n^2,1-1/n^2}$$

We can therefore conclude that $IID^{a,b'}$ is complete for $NISZK_{|h}$ when $b' > 2a$. □