1 Introduction

Consider a case where you (as a prover) want to prove to your friend (called verifier) that you know a solution \( w \) to some problem \( x \) without revealing the solution itself, i.e., \((x, w) \in R\). In cryptography, it means that you need to give a zero-knowledge proof (of knowledge).

Zero-knowledge proofs are interactive proofs with the special property that the verifier does not learn anything except that the statement is valid. Furthermore, zero-knowledge proofs are one of the most powerful techniques of cryptographers.

In this report, we study the problem of quantum zero-knowledge based on [1] and [2]. In the classical setting, zero-knowledge proofs use rewinding technique to construct an extractor which extracts the witness \( w \) from the prover. In the quantum setting, classical rewinding is impossible: measuring a quantum state in superposition fixes the state. In order to overcome this issue clever quantum rewinding techniques have been introduced. The goal of this report is to show that quantum honest verifier zero-knowledge \( \Sigma \)-protocols are also quantum computational zero knowledge.

We begin in Section 2 with describing the concept of zero-knowledge and introducing the basics of quantum systems. This is followed in Section 3 with presenting the problem of quantum zero-knowledge and a proof for quantum computational zero knowledge.

2 Preliminaries

In this section, we introduce the notation and definitions used in this report. We mainly follow [1]. We begin with essential definitions and notation to understand quantum systems. This is followed by necessary definitions to explain the concept of zero-knowledge proofs. We note that we do not focus in this report on zero-knowledge proofs of knowledge, following definitions are necessary to understand the overall concept.
2.1 Quantum Systems

A single qubit is represented as a vector $|\Psi\rangle \in \mathbb{C}^2$, and its (Euclidean) norm is denoted by $|||\Psi\rangle||$. It holds that $|||\Psi\rangle|| = 1$.

Consider a state $|\Psi\rangle = \sum_{i=1}^{m} p_i |\Psi_i\rangle$ where $\sum_{i=1}^{m} |p_i|^2 = 1$. The latter is a superposition of orthonormal vectors $|\Psi_i\rangle$, i.e., during measurement $|\Psi\rangle$ obtains one of these values $|\Psi_i\rangle$ and the probability of obtaining value $|\Psi_i\rangle$ is equal to $p_i^2$. We call a basis computational if it is a canonical orthonormal basis of $\mathbb{C}^n$.

There are two kinds of operations, measurements and unitary transformations. A unitary transformation (on a single qubit) is a transformation described by a unitary matrix $U \in \mathbb{C}^{2 \times 2}$. It holds that $UU^\dagger = U^\dagger U = I$, where $U^\dagger$ denotes the complex conjugate of the transposition of $U$. After applying $U$ to a qubit $|\Psi\rangle$, we have that the resulting state is $U|\Psi\rangle$.

Definition 2.1 (Quantum ensemble). A quantum ensemble $E$ over Hilbert space $\mathcal{H}$ is a set of pairs $E = \{|\Phi_i\rangle, p_i\}_i$ satisfying the following:

- $\forall i$ we have $|\Phi_i\rangle \in \mathcal{H}$,
- $\forall i$ we have $|||\Phi_i\rangle|| = 1$,
- $\forall i$ we have $p_i \geq 0$ and $\sum_i p_i = 1$.

In the definition above, we have that with probability $p_i$ the system is in state $|\Phi_i\rangle$.

Definition 2.2 (Density operator). Let $E = \{|\Phi_i\rangle, p_i\}_i$ be a quantum ensemble over $\mathcal{H}$. The density operator corresponding to $E$ is linear transformation $\rho_E = \sum_i p_i |\Phi_i\rangle \langle \Phi_i|$.

In the following, denote the absolute value matrix of $A$ by $|A|$ and by $tr.A$ its trace value.

Definition 2.3 (Trace distance). Given density operators $\sigma, \rho \in S(\mathcal{H})$, we define the trace distance between $\sigma$ and $\rho$ as

$$TD(\sigma, \rho) := \frac{1}{2}tr|\sigma - \rho|.$$  

2.2 Zero-Knowledge Proofs

In this report, we denote a proof system for relation $R$ by $(P, V)$, where $P$ we call prover and $V$ verifier. We say that a conversation between prover and verifier is accepting if $\langle P(x, w), V(x) \rangle = 1$ where $(x, w)$ is prover’s input and $(x)$ is verifier’s input.
**Definition 2.4 (Σ-protocol).** A proof system $(P, V)$ is called a Σ-protocol (sigma-protocol) if $P$ and $V$ are classical, the interaction consists of three messages $\alpha$; $\beta$; $\gamma$ (sent by $P$, $V$ and $P$, respectively, and called commitment, challenge, and response), where $\beta$ is uniformly chosen from set $C_{\eta x}$ (the challenge space, denote sampling as $\beta \leftarrow C_{\eta x}$) that may only depend on the statement $x$ and the security parameter $\eta$. Furthermore, the verifier decides whether to accept or not by a deterministic polynomial-time computation $x$, $\alpha$; $\beta$; $\gamma$. We also require that it is possible in probabilistic polynomial time to sample uniformly from $C_{\eta x}$ up to negligible error, and that membership in $C_{\eta x}$ should be decidable given $\eta$, $x$ in deterministic polynomial time in $\eta + |x|$.

Σ-protocol can have many different properties, i.e., depending on the property one can construct e.g., proofs of knowledge and zero-knowledge proofs of knowledge. Next, we define some properties.

**Definition 2.5 (Soundness).** A Σ-protocol $(P, V)$ for a relation $R$ is sound with soundness error $0 \leq s \leq 1$ if for all malicious provers $P^*$, all $\eta \in \mathbb{N}$, all auxiliary inputs $r$, and all $x$ for which there does not exist $w$ such that $(x, w) \in R$, we have $\Pr [\langle P^*(x, r), V(x) \rangle = 1] \leq s(\eta)$.

**Definition 2.6 (Completeness).** A Σ-protocol $(P, V)$ for a relation $R$ is complete if there is a negligible function $\mu$ such that for all $\eta \in \mathbb{N}$ and all $(x, w) \in R$, we have that $\Pr [\langle P(x, w), V(x) \rangle = 1] \geq 1 - \mu(\eta)$.

**Definition 2.7 (Special soundness).** A Σ-protocol $(P, V)$ for a relation $R$ is specially sound if there is a deterministic polynomial-time algorithm $K_0$ (the special extractor) such that the following holds: For any two accepting conversations $(\alpha, \beta, \gamma)$ and $(\alpha, \beta', \gamma')$ for $x$ such that $\beta \neq \beta'$ and $\beta, \beta' \in C_{\eta x}$, we have that $w := K_0(x; \alpha, \beta, \gamma, \beta', \gamma')$ satisfies $(x, w) \in R$.

Observe that special soundness property of a Σ-protocol allows one to construct the witness $w$. Furthermore, if Σ-protocol is specially sound, it follows that the protocol is also sound.

Note that the prover may not produce two distinct accepting conversations to run with the extractor. If that is the case, we can construct an extractor $K$ which uses $K_0$ and runs a prover $P^*$ itself. Then $K$ runs $P^*$ using a challenge $\beta$. After it produces an accepting response $\gamma$, then the extractor rewrites $P^*$ to the point before it received $\beta$. Then the extractor runs $P^*$ on another input $\beta' \neq \beta$ and obtains an accepting response $\gamma'$. Then, $K$ uses $K_0$ on $x, \alpha, \beta, \gamma, \beta', \gamma'$ and obtains the witness $w$. In the following, we denote such extractor by $K^{P^*}$.

In classical setting, zero-knowledge proofs use rewinding technique to construct the extractor which extracts the witness from the prover. Namely, it is possible to construct an extractor $K^{P^*}$ which creates $w$ for $x$ such that $(x, w) \in R$ holds. The idea is that prover $P^*$ is rewinded, meaning it does not learn anything about the previous execution.
Therefore, for $\beta$ and $\beta'$ ($\beta' \neq \beta$) it is possible to construct $\gamma$ and $\gamma'$ such that it can recover $w$.

In quantum setting classical rewinding is impossible: measuring a state in superposition fixes the state. The extractor $K^{P^*}$ runs $P^*$ to obtain $\alpha$ gives it $\beta$ and runs the next step of $P^*$, and measures $\gamma$. Rewinding can be modelled as a unitary (inverse operation of the previous step) transformation back to the state before sending $\beta$. It then gives $P^*$ another $\beta'$, $\beta' \neq \beta$ and runs a single step and finally measures $\gamma'$. However, for the classical prover, if the extractor obtains $\beta$, it did not disturb $P^*$, then for the quantum case it could disturb the internal state of $P^*$ if it is in a superposition, invalidating the probability of having two accepting conversations. We refer the interested reader to [1] for specific constructions.

A $\Sigma$-protocol $(P, V)$ with completeness and special soundness is a classical proof of knowledge. Protocol that is only proof of knowledge is not sufficient. We want protocol to be zero-knowledge. Finally, we are ready to define honest-verifier zero-knowledge for the classical case.

**Definition 2.8** (Honest-verifier zero-knowledge (HVZK)). A $\Sigma$-protocol $(P, V)$ honest-verifier zero-knowledge if there is a polynomial-time algorithm $S_\Sigma$ (the simulator) such that the transcript of the interaction $(P(x, w), V(x))$ is computationally indistinguishable from the output of $S_\Sigma(x)$. Namely, we require that there exists a polynomial-time $S_\Sigma$ such that for any polynomial- time $D_\Sigma$ and any polynomial $l$, there is a negligible $\mu$ such that for all $(x, w) \in R$ with $|x|, |y| \leq l(\eta)$, and for all states $r$:

$$\left| \Pr[b = 1 : (\alpha, \beta, \gamma) \leftarrow (P(x, w), V(x)), b \leftarrow D_\Sigma(r, \alpha, \beta, \gamma)] - \Pr[b = 1 : (\alpha, \beta, \gamma) \leftarrow S_\Sigma(x), b \leftarrow D_\Sigma(r, \alpha, \beta, \gamma)] \right| \leq \mu(\eta).$$

The intuition behind the HVZK property defined above is to guarantee that the verifier does not learn anything about the witness $w$ because it cannot distinguish between the protocol execution between the actual prover and the simulator.

$\Sigma$-protocol with completeness, special soundness and HVZK is a zero-knowledge proof of knowledge.

### 3 Quantum Zero-Knowledge

Let us begin with formally defining quantum honest-verifier zero-knowledge. It is an analogue of the classical case.

**Definition 3.1** (Honest-verifier zero-knowledge (HVZK)). A $\Sigma$-protocol $(P, V)$ is honest-verifier zero-knowledge if there is a quantum-polynomial-time algorithm $S_\Sigma$ (the simulator) such that the transcript of the interaction $(P(x, w), V(x))$ quantum-computationally indistinguishable from the output of $S_\Sigma(x)$. Namely, we require that there exists a
quantum-polynomial-time $S_{\Sigma}$ such that for any quantum-polynomial-time $D_{\Sigma}$ and any polynomial $l$, there is a negligible $\mu$ such that for all $(x, w) \in R$ with $|x|, |y| \leq l(\eta)$, and for all states $|\Psi\rangle$:

$$\left| \Pr[b = 1 : (\alpha, \beta, \gamma) \leftarrow \langle P(x, w), V(x) \rangle, b \leftarrow D_{\Sigma}(|\Psi\rangle, \alpha, \beta, \gamma) \right] \right. - \Pr[b = 1 : (\alpha, \beta, \gamma) \leftarrow S_{\Sigma}(x), b \leftarrow D_{\Sigma}(|\Psi\rangle, \alpha, \beta, \gamma)] \right| \leq \mu(\eta).$$

In the definition above, $S_{\Sigma}$ is quantum. Quantum computational zero-knowledge is defined as follows:

**Definition 3.2 (Quantum computational ZK).** An interactive proof system $(P, V)$ for relation $R$ is quantum computational zero-knowledge iff for every quantum-polynomial-time verifier $V^*$ there is a quantum-polynomial-time simulator $S$ such that for any quantum-polynomial-time distinguisher $D$ and polynomial $l$ there is a negligible $\mu$ such that for any $(x, w) \in R$ with $|x|, |w| \leq l(\eta)$, and for any quantum state $|\Psi\rangle$, we have that

$$\left| \Pr[b = 1 : ZE \leftarrow |\Psi\rangle, \langle P(x, w), V^*(Z) \rangle, b \leftarrow D(Z, E) \right] \right. - \Pr[b = 1 : ZE \leftarrow |\Psi\rangle, S(x, Z), b \leftarrow D(Z, E)] \right| \leq \mu(\eta).$$

In the definition above, $ZE \leftarrow |\Psi\rangle$ means that registers $Z$ and $E$ are initialized jointly with state $|\Psi\rangle$, $V^*(Z)$ and $S(x, Z)$ mean that verifier $V^*$ and simulator $S$ both have access to quantum register $Z$. Note that having access implies that the state may change.

Furthermore, in [2] it is assumed, that the honest prover has to find witness $w$ himself, but in the definition above honest prover is given access to the witness. Otherwise, we could have efficient honest provers only for trivial languages.

The following is a reformulation from [11] of quantum rewinding technique introduced in [2].

**Corollary 3.3 (Quantum Rewinding Lemma with small perturbations).** Let $C, Z, E$ and $Y$ be quantum registers where $C$ is one qubit register. Let $S_1$ be unitary transformation operating on $C, Z, Y$ and let $M$ be a measurement in the computational basis on $C$.

For a quantum state $|\Psi\rangle$, let $p(|\Psi\rangle) := \Pr[\text{succ} = 1 : S_1(CZY), \text{succ} \leftarrow M(C)]$ where $Z$ and $E$ are jointly initialized with $|\Psi\rangle$, and $Y$ and $C$ are initialized with $|0\rangle$. Let $\rho^1_{\Psi}$ denote the state of $ZE$ when $\text{succ} = 1$.

Let $\varepsilon \in (0, \frac{1}{2})$ and $q \in (\varepsilon, \frac{1}{2}]$. Assume that for all $|\Psi\rangle$, $|p(|\Psi\rangle) - q| \leq \varepsilon$.

Then, there exists a quantum circuit $S$ operating on $Z$ of size $O(k := \log(1/\varepsilon)/\log(1-(q-\varepsilon)))$. $S$ is a general quantum circuit which can create auxiliary qubits, destroy them and perform measurements. $S$ can be computed in time $k$ given the description of $S_1$. For any $|\Psi\rangle$,

$$\text{TD}(\rho^1_{\Psi}, \rho^2_{\Psi}) \leq 4\sqrt{\varepsilon \frac{k}{\text{size}(S_1)}}.$$
where \( \rho^\beta_q \) denotes the state of \( ZE \) after execution of \( S \).

**Proof.** We refer the interested reader to [1] and omit the proof. \qed

Next, we are ready to present the main theorem of quantum zero-knowledge.

**Theorem 3.4.** Let \( (P, V) \) be a \( \Sigma \)-protocol. Assume that \( P \) gives some fixed error \( \text{err} \) when receiving \( \beta \notin C_{\eta x} \) as input. If \( C_{\eta x} \) is polynomially bounded in \( \eta + |x| \) and \( \Sigma \) is HVZK, then \( (P, V) \) is quantum computational zero-knowledge.

**Proof.** W.l.o.g., we assume that we never have \( \text{HVZK} \), then \( \text{HVZK} \) holds if and only if \( (P, V) \) is quantum computational zero-knowledge.

We represent prover \( P \) with two algorithms \( P_1 \) and \( P_2 \) such that \( \alpha \leftarrow P_1(x, w) \) and \( \gamma \leftarrow P_2(x, w, \beta) \). \( P_1 \) and \( P_2 \) can share a state. Similarly, we represent \( V^* \) with two algorithms \( V_1^* \) and \( V_2^* \) such that \( \beta \leftarrow V_1^*(\alpha, \gamma) \) and \( V_2^*(\gamma, \gamma) \), again \( V_1^* \) and \( V_2^* \) can share a state.

Therefore, \( \langle P(x, w), V^*(Z) \rangle \) is equal to

<table>
<thead>
<tr>
<th>Prover</th>
<th>Verifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \alpha \leftarrow P_1(x, w) )</td>
<td>( \beta \leftarrow V_1^*(\alpha, Z) )</td>
</tr>
<tr>
<td>( \gamma \leftarrow P_2(x, w, \beta) )</td>
<td>( V_2^*(\gamma, Z) )</td>
</tr>
</tbody>
</table>

As \( \Sigma \) is HVZK (see Definition 3.1), there exists a quantum polynomial-time simulator \( S_\Sigma \) such that for any quantum polynomial-time \( D_\Sigma \) we have that

\[
\begin{align*}
\Pr[b = 1 : \alpha \leftarrow P_1(x, w), \beta \leftarrow C_{\eta x}, \gamma \leftarrow P_2(x, w, \beta), b \leftarrow D_\Sigma(|\Psi\rangle, \alpha, \beta, \gamma)]
- \Pr[b = 1 : (\alpha, \beta, \gamma) \leftarrow S_\Sigma(x), b \leftarrow D_\Sigma(|\Psi\rangle, \alpha, \beta, \gamma)] &\leq \varepsilon_D(\eta).
\end{align*}
\]

Denote \([\beta = \beta'] := 1 \iff \beta = \beta'\). Therefore, we have that

\[
\begin{align*}
&\Pr[\text{succ} = 1 \land b = 1 : ZE \leftarrow |\Psi\rangle, \langle P(x, w), V^*(Z) \rangle, b \leftarrow D(Z, E), \beta' \leftarrow C_{\eta x}, \\
&\text{succ} := [\beta = \beta']] = \\
&\Pr[\text{succ} = 1 \land b = 1 : ZE \leftarrow |\Psi\rangle, \alpha \leftarrow P_1(x, w), \beta \leftarrow V_1^*(\alpha, Z), \gamma \leftarrow P_2(x, w, \beta), \\
&V_2^*(\gamma, Z), b \leftarrow D(Z, E), \beta' \leftarrow C_{\eta x}, \text{succ} := [\beta = \beta']] = \\
&\Pr[\text{succ} = 1 \land b = 1 : \alpha \leftarrow P_1(x, w), \beta' \leftarrow C_{\eta x}, \gamma \leftarrow P_2(x, w, \beta'), ZE \leftarrow |\Psi\rangle \\
&\beta \leftarrow V_1^*(\alpha, Z), \text{succ} := [\beta = \beta'], V_2^*(\gamma, Z), b \leftarrow D(Z, E)] \approx \\
&\Pr[\text{succ} = 1 \land b = 1 : (\alpha, \beta', \gamma) \leftarrow S_\Sigma(x), ZE \leftarrow |\Psi\rangle \\
&\beta \leftarrow V_1^*(\alpha, Z), \text{succ} := [\beta = \beta'], V_2^*(\gamma, Z), b \leftarrow D(Z, E)] = \\
&\Pr[\text{succ} = 1 \land b = 1 : ZE \leftarrow |\Psi\rangle, Y, C \leftarrow |0\rangle, S_1(x, CZY), \\
&succ \leftarrow M(C), b \leftarrow D(Z, E)].
\end{align*}
\]
First, we use the fact that $P_2(x, w, \beta)$ and $P_2(x, w, \beta')$ get the same arguments when $\beta = \beta'$.

Then, we have that a quantum-polynomial-time $D_\Sigma(\langle \Psi \rangle, \alpha, \beta, \gamma)$ runs

$$ZE \leftarrow \langle \Psi \rangle, \beta \leftarrow V_1^*(\alpha, Z), \text{succ} := [\beta = \beta'], V_2^*(\gamma, Z), b \leftarrow D(Z, E)$$

returning $b \land \text{succ}$, i.e., probabilities are $\varepsilon$ close.

This is followed by constructing a unitary quantum circuit $S_1$: we transform

$$(\alpha, \beta', \gamma) \leftarrow S_\Sigma(x), ZE \leftarrow \langle \Psi \rangle, \beta \leftarrow V_1^*(\alpha, Z), \text{succ} := [\beta = \beta'], V_2^*(\gamma, Z)$$

into a unitary quantum circuit which operates on registers $C, Z$ and $Y$. We store the value of $\text{succ}$ in the one-qubit register $C$ and retrieve the value $\text{succ} \leftarrow M(C)$ by performing measurement $M$ on $C$ in the computational basis.

Observe that for all quantum states $\langle \Psi \rangle$, we have that

$$\frac{1}{|C_{\eta x}|} = \Pr[\text{succ} = 1 : ZE \leftarrow \langle \Psi \rangle, \langle P(x, w), V^*(Z) \rangle, \beta' \leftarrow C_{\eta x}, \text{succ} := [\beta = \beta']]$$

$$\approx \Pr[\text{succ} = 1 : ZE \leftarrow \langle \Psi \rangle, Y, C \leftarrow |0 \rangle, S_1(x, CZY), \text{succ} \leftarrow M(C)].$$

The discussion why the above holds is similar to (1). We omit this here due to technicality.

In the following, w.l.o.g., we take $\varepsilon' \geq \frac{1}{2\eta}$. Observe that as we assume $|C_{\eta x}|$ to be polynomially bounded in $\eta + |x|$, and $|x| \leq l(\eta)$, thus, $q := \frac{1}{|C_{\eta x}|}$ is noticeable in $\eta$.

Following Corollary 3.3, we have that there exists an algorithm $S$ such that for sufficiently large $\eta$

$$\text{TD}(\rho_1^1, \rho_2^2) \leq 4\sqrt{\varepsilon'} \frac{\eta}{(q - \varepsilon')(1 - q + \varepsilon')} := \delta,$$

where $\rho_1^1$ is the final state of $ZE$ after executing

$$S_1(x, CZY), \text{succ} \leftarrow M(C)$$

and having $\text{succ} = 1$, and $\rho_2^2$ is the final state of $ZE$ after executing

$$S(x, CZY).$$

In Corollary 3.3 we assume that $q > \varepsilon$, since $q$ is noticeable and $\varepsilon$ is negligible, this is achieved for sufficiently large $\eta$.

Observe that the running time of the algorithm is polynomially-bounded as size of $S_1$ is polynomially bounded, $q - \varepsilon$ is noticeable and $q \leq \frac{1}{2}$. 7
Therefore, as two states cannot be distinguished better than their trace distances, we have that

\[
\Pr[b = 1 : ZE \leftarrow |\Psi\rangle, Y, C \leftarrow |0\rangle, S_1(x, CZY), succ \leftarrow M(C), b \leftarrow D(Z, E) | succ = 1] \approx \Pr[b = 1 : ZE \leftarrow |\Psi\rangle, Y, C \leftarrow |0\rangle, S(x, CZY), b \leftarrow D(Z, E)]
\]

Next, we need to use Claim 3.5. Suppose that \( B \) is the event \( b = 1 \), and \( S \) is the event \( succ = 1 \). \( \Pr_1 \) refers to the probability space defined by

\[
ZE \leftarrow |\Psi\rangle, \langle P(x, w), V^*(Z) \rangle, b \leftarrow D(Z, E), \beta' \leftarrow C_{\eta x}, succ := [\beta = \beta'],
\]

and \( \Pr_2 \) refers to the probability space defined by

\[
ZE \leftarrow |\Psi\rangle, Y, C \leftarrow |0\rangle, S_1(x, CZY), succ \leftarrow M(C), b \leftarrow D(Z, E).
\]

Observe that \( B \) and \( S \) are independent in \( \Pr_1 \). Furthermore, we have that \( \Pr_1[B \wedge S] \approx \Pr_2[B \wedge S] \) and \( \Pr_1[S] \approx \Pr_2[S] \). Also, as \( \Pr_1[S] = 1/|C_{\eta x}| \), we have

\[
\Pr[b = 1 : ZE \leftarrow |\Psi\rangle, \langle P(x, w), V^*(Z) \rangle, b \leftarrow D(Z, E) | succ = 1] \approx \Pr[b = 1 : ZE \leftarrow |\Psi\rangle, S(x, Z), b \leftarrow D(Z, E)],
\]

where simulator \( S(x, Z) \) runs

\[
Y, C \leftarrow |0\rangle, S(x, CZY).
\]

As simulator \( S \) is quantum polynomial-time, \( \varepsilon, \varepsilon' \) and \( \delta \) are negligible, and \( |C_{\eta x}| \) is polynomially bounded, Definition 3.2 holds and equation is bounded by \( |C_{\eta x}|(\varepsilon + \varepsilon') + \delta \). Thus, we have shown that \( \Sigma \) is quantum computational zero-knowledge.

\[
\square
\]

**Claim 3.5 (Claim 3).** Consider two probability spaces \( \Pr_1, \Pr_2 \) with events \( B \) and \( S \). Assume that the latter events are independent in \( B \) and \( S \). Assume that \( \Pr_1[B \wedge S] \approx \Pr_2[B \wedge S] \) and \( \Pr_1[S] \approx \Pr_2[S] \), then \( \Pr_1[B] \approx \Pr_2[B | S] \).

### 4 Conclusion

In this report, we studied the concept of quantum zero-knowledge based on [1] and [2]. We showed that quantum computational zero-knowledge does exist, namely that honest verifier zero-knowledge implies quantum computational zero-knowledge.
References
