

TQC 2006

# Statistical Zero Knowledge and Quantum One-way Functions

Elham Kashefi

February 22, 2006

IQC - University of Waterloo

*(Joint work with Iordanis Kerenidis)*

- ▶ Fundamental task of cryptography: secure encryption of information against malicious parties (One-way functions)
- ▶ Theoretical applications: bit commitment and oblivious transfer, Zero Knowledge Proof Systems and pseudo-random generators
- ▶ Candidate one-way functions: Factoring, Discrete Logarithm, Graph Isomorphism, Quadratic Residuosity, approximate Shortest Vector and Closest Vector and the RSA function

# Emergence of Quantum Computation

- ▶ Possibility of unconditionally secure key distribution
- ▶ Classical one-way functions and hence cryptosystems, including RSA, will not be secure against quantum adversaries

# Motivations

- ▶ Constructing cryptosystems secure even against quantum attacks
- ▶ Candidates for quantum one-way functions
- ▶ Quantum analogues of the “classic” results on 1way functions

- ▶ Quantum computationally secure bit commitment  
*DumaisMS00, CrépeauLS01, AdcockC01*
- ▶ Digital signature schemes (Classical inputs and quantum outputs) *GottesmanC01, Yuen00, LuF04*
- ▶ Testing the one-wayness based on the efficiency of constructing a family of reflection operators  
*KashefiNV02, KawachiKKP04*

# Summary

- ▶ Quantum Sampling  $\longrightarrow$  quantum 1way functions
- ▶ Quantum distributionally 1way  $\longrightarrow$  quantum 1way functions
- ▶ Candidate functions:
  - $\mathcal{L} \in SZK \setminus AvgBQP$
  - $\mathcal{L} \in QMA\text{-Intermediate}$

## Definition

A one to one function  $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$  where:

- ▶ easy to compute:  $f$  can be computed by a polynomial size classical network
- ▶ hard to invert:  $\exists$  a polynomial  $p(\cdot)$  such that  $\forall$  poly. time quantum algorithm  $I$  and all sufficiently large  $n \in \mathbb{N}$ ,

$$\frac{1}{2^n} \sum_{x \in \{0,1\}^n} \text{Prob}[I(f(x)) \notin f^{-1}(f(x))] > \frac{1}{p(n)}$$

## Definition

A one to one function  $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$  where:

- ▶ easy to compute:  $f$  can be computed by a polynomial size classical network
- ▶ hard to invert:  $\exists$  a polynomial  $p(\cdot)$  such that  $\forall$  poly. time quantum algorithm  $I$  and all sufficiently large  $n \in \mathbb{N}$ ,

$$\frac{1}{2^n} \sum_{x \in \{0,1\}^n} \text{Prob}[I(f(x)) \in f^{-1}(f(x))] \leq 1 - \frac{1}{p(n)}$$

- ▶ Closeness of the outcome of  $I$  and the outcome of the perfect inverter  $P$ , where

$$P : |f(x)\rangle|0\rangle \mapsto |f(x)\rangle|x\rangle$$

- ▶ For the case of one-to-one functions

$$\begin{aligned} \text{Prob}[I(f(x)) \in f^{-1}(f(x))] &= \text{Prob}[I(f(x)) = x] \\ &= |\langle I(|f(x)\rangle|0\rangle, |f(x)\rangle|x\rangle|^2 \end{aligned}$$

# Equivalent Definition

To demonstrate the relation between quantum one-way functions and the Quantum Sampling:

# Equivalent Definition

To demonstrate the relation between quantum one-way functions and the Quantum Sampling:

## Definition

...

- ▶ hard to invert:  $\exists$  a polynomial  $p(\cdot)$  such that  $\nexists$  poly. time quantum algorithm  $I'$  that for all sufficiently large  $n \in \mathbb{N}$ :

$$I' : |f(x)\rangle|0\rangle \mapsto a_{f(x)}|f(x)\rangle|x\rangle + b_{f(x)}|f(x)\rangle|G_{f(x)}\rangle \quad (1)$$

where  $G_{f(x)}$  is a garbage state,  $\frac{1}{2^n} \sum_{x \in \{0,1\}^n} a_{f(x)}^2 \geq 1 - \frac{1}{p(n)}$  and  $a_{f(x)}$  are positive real numbers.

- ▶ By copying the input in an entangled register we make the garbage state orthogonal to the correct state
- ▶ By running twice the inverting algorithm and assuming, without loss of generality, that the initial amplitudes were real numbers, we can make the amplitudes positive real numbers

- ▶ To prepare efficiently a certain superposition state
- ▶ We restrict ourselves to superpositions that correspond to samplable classical probability distributions

# Quantum Sampling of a classical circuit $C$

- ▶  $D_C$  be the distribution over outputs of  $C$
- ▶  $|C\rangle = \sum_{z \in \{0,1\}^m} \sqrt{D_C(z)} |z\rangle$

## Definition (Aharonov and Ta-shma)

CQS problem: For a given  $C$  find a quantum circuit of size  $\text{poly}(|C|)$  which prepares the quantum sample  $|C\rangle$ :

$$|QS_C(|0\rangle) - |C\rangle| \leq \epsilon$$

## Theorem

*Assume for a classical circuit  $C$ , which computes a one-to-one function, the corresponding CQS problem is hard, then the function  $f_C : x \mapsto C(x)$  is a quantum one-way function.*

From  $C$  we obtain  $U_f : |x\rangle|b\rangle \mapsto |x\rangle|f(x) \oplus b\rangle$

Assume  $f$  is not one-way:  $\forall p \exists I'$  which inverts  $f$  approximately:

$$I' : |f(x)\rangle|0\rangle \mapsto a_{f(x)}|f(x)\rangle|x\rangle + b_{f(x)}|f(x)\rangle|G_{f(x)}\rangle$$

where  $|G_{f(x)}\rangle$  is a garbage state and  $\frac{1}{2^n} \sum_x a_{f(x)}^2 > 1 - \frac{1}{p(n)}$ .

we can construct the following circuit  $QS_C$ :

$$\begin{aligned}
 |x\rangle|0\rangle &\Rightarrow_{U_f} |x\rangle|f(x)\rangle \\
 &\Rightarrow_{SWAP} |f(x)\rangle|x\rangle \\
 &\Rightarrow I' a_{f(x)}|f(x)\rangle|0\rangle + b_{f(x)}|f(x)\rangle|G_{f(x)}\rangle
 \end{aligned}$$

Starting with a uniform superposition of  $x \in \{0, 1\}^n$  we have

$$\begin{aligned}
 \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle|0\rangle &\Rightarrow_{QS_C} \\
 \frac{1}{2^{n/2}} \sum_x ( a_{f(x)}|f(x)\rangle|0\rangle + b_{f(x)}|f(x)\rangle|G'_{f(x)}\rangle ) &\equiv Q
 \end{aligned}$$

Let  $|C\rangle = \frac{1}{2^{n/2}} \sum_x |f(x)\rangle|0\rangle$  be the quantum sample of the circuit

$$\begin{aligned} |(Q, |C\rangle)|^2 &= \left| \frac{1}{2^n} \sum_x a_{f(x)} \right|^2 \\ &\geq \left| \frac{1}{2^n} \sum_x a_{f(x)}^2 \right|^2 \\ &> (1 - 1/p(n))^2 \\ &> 1 - \epsilon \end{aligned}$$

# Many-to-one Case

Our result extends to the many-to-one functions with the assumption that the inverting algorithm for the one-way function provides a uniform superposition of the preimages of  $f$ .

# Quantum distributionally one-way function

## Definition

A many-to-one function  $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$  where:

- ▶ easy to compute:  $f$  can be computed by a polynomial size classical network.
- ▶ hard to sample: There exists a polynomial  $p(\cdot)$  such that for any quantum polynomial time algorithm  $S$  and all sufficiently large  $n \in \mathbb{N}$ ,

$$\frac{1}{2^n} \sum_{x \in \{0,1\}^n} |(S(|f(x)\rangle|0\rangle), |f(x)\rangle|H_{f(x)}\rangle)|^2 \leq 1 - \frac{1}{p(n)},$$

where  $|H_{f(x)}\rangle = \frac{1}{\sqrt{|f^{-1}(f(x))|}} \sum_{x \in f^{-1}(f(x))} |x\rangle$ .

## Theorem

*Assume for a classical circuit  $C$ , which computes a many-to-one function, the corresponding CQS problem is hard, i.e. there exists no  $\text{poly}(|C|)$  size quantum circuit implementing  $QS_C$ . Then the function  $f_C : x \mapsto C(x)$  is a quantum distributionally one-way function.*

# Sampling vs Inverting

## Theorem (Luby and Impagliazzo)

*if  $\exists$  a distributional one-way function then  $\exists$  a general one-way function.*

# Sampling vs Inverting

## Theorem (Luby and Impagliazzo)

*if  $\exists$  a distributional one-way function then  $\exists$  a general one-way function.*

- ▶ Assume  $f$  is dist. 1way and we know the size of the preimage,  $k = \lfloor \log |f^{-1}(f(x))| \rfloor + O(\log n)$  Then the following function is 1way:

$$g(x, h_k) = (f(x), h_k, h_k(x))$$

where  $h_k$  is a random hash function  $h_k : \{0, 1\}^n \rightarrow \{0, 1\}^k$ .

## Theorem

*if  $\exists$  a quantum distributional one-way function then  $\exists$  a general quantum one-way function.*

- ▶ Assume, we know the  $k = \lceil \log |f^{-1}(f(x))| \rceil + O(\log n)$
- ▶ Picking a random hash function and a random string

$$Q : |k\rangle|0\rangle \rightarrow |k\rangle \sum_{h_k} |h_k\rangle \quad , \quad B : |k\rangle|0\rangle \rightarrow |k\rangle \sum_{r_k} |r_k\rangle$$

- ▶ Quantum inverter of  $g$  as

$$I : \left\{ \begin{array}{ll} |f(x)\rangle|h_k\rangle|h_k(x)\rangle|0\rangle|0\rangle & \rightarrow_{\epsilon} |f(x)\rangle|h_k\rangle|h_k(x)\rangle|x\rangle|0\rangle \\ |f(x)\rangle|h_k\rangle|s_k\rangle|0\rangle|0\rangle & \rightarrow |f(x)\rangle|h_k\rangle|s_k\rangle|0\rangle|1\rangle \end{array} \right\}$$

$$T : |h_k\rangle|h_k(x)\rangle|x\rangle \rightarrow |h_k\rangle|0\rangle|x\rangle$$

## Partial Quantum Sampler PQS( $f(x),k$ )

$$|f(x)\rangle|k\rangle|0\rangle|0\rangle|0\rangle \Rightarrow$$

$$\sqrt{p_k}|f(x)\rangle|k\rangle|0\rangle|0\rangle|H_{f(x)}\rangle|0\rangle + \sqrt{1-p_k}|f(x)\rangle|k\rangle|G_{f(x),k}\rangle|1\rangle$$

**Partial Ancilla Preparation, PAP( $f(x),k$ )**

$$|f(x)\rangle|k\rangle|0\rangle|0\rangle|0\rangle \Rightarrow$$

$$|f(x)\rangle|k\rangle\left(p_k|0\rangle + (1 - p_k)|1\rangle\right)|0\rangle + |f(x)\rangle|G_{f,k}\rangle|1\rangle$$

**Ancilla Preparation AP(f(x))**

$$|f(x)\rangle|n\rangle|0\rangle|n-1\rangle|0\rangle \cdots |1\rangle|0\rangle|0\rangle \Rightarrow$$

$$|f(x)\rangle|n\rangle \cdots |1\rangle \sum_j q_j |j\rangle|0\rangle + |G_f\rangle|1\rangle$$

where  $q_j = \prod_{i=1}^{j-1} (1 - p_i) p_j$

**Quantum Sampler, QS(f(x))**

$$|f(x)\rangle|0\rangle|0\rangle \Rightarrow$$

$$\sum_j q_j^2 \sqrt{p_j} |f(x)\rangle |H_{f(x)}\rangle |0\rangle + |G_{f(x)}\rangle |1\rangle$$

- ▶ Our main theorem provides a framework for seeking candidates
- ▶ Quantum states hard to generate  $\Rightarrow$  the intractability of inversion
- ▶ Classically samplable distribution  $\Rightarrow$  the ability to generate instances together with the auxiliary information

# Statistical Zero Knowledge

- ▶ *SZK* proof: To prove an statement without yielding anything beyond its validity.
- ▶ *SZK* language: There is a *SZK* interactive proof system to decide it, (verifier can learn only about  $x \in L$ ).

- ▶ (Aharonov Tash-ma 03) Any language  $\mathcal{L} \in SZK$  can be reduced to a family of instances of CQS problem.
- ▶ (Sahami and Vadhan 99) Consider two constants  $0 \leq \beta < \alpha \leq 1$  such that  $\alpha^2 > \beta$ , define  $SD_{\alpha,\beta}$  to be the problem of deciding for any two given classical circuits  $C_0$  and  $C_1$  whether:

$$\begin{aligned} \|D_{C_0} - D_{C_1}\| &\geq \alpha && \text{or} \\ \|D_{C_0} - D_{C_1}\| &\leq \beta \end{aligned}$$

where it is promised one to occur.

The quantum analogue of Ostrovsky's result:

## Theorem

*Assume there exists a language  $\mathcal{L} \in \text{SZK} \setminus \text{AvgBQP}$ , then quantum one-way functions exist.*

The quantum analogue of Ostrovsky's result:

## Theorem

*Assume there exists a language  $\mathcal{L} \in \text{SZK} \setminus \text{AvgBQP}$ , then quantum one-way functions exist.*

Proof. Assume  $\mathcal{L} \in \text{SZK} \setminus \text{AvgBQP}$  and let  $C_0$  and  $C_1$  be the classical circuits which decide  $L$  via reduction to the SV-complete language. Then either of the corresponding functions  $f_0$  or  $f_1$  is quantum one-way.

# Conclusions

- ▶ Hard instances of q. sampling  $\Rightarrow$  q. one-way functions  
Easy instances  $\Rightarrow$  efficient quantum algorithms
- ▶  $SZK \not\subseteq AvgBQP \Rightarrow$  Hard instances  
*What other assumptions  $\Rightarrow$  hard instances of the CQS?*
- ▶ Candidate one-way problems: Graph Non-Isomorphism and approximate Closest Lattice Vector problem  
*Can we construct one-way functions from other problems, such as the hidden subgroup problem in the dihedral or other non-abelian groups?*
- ▶ Watrous proved q. one-way functions  $\Rightarrow$  computational zero knowledge for NP  
*Other such implications?*