Lecture 22

Motivating a Quantum Digital Signature Algorithm

of the course "Fundamentals of Quantum Computing"
(by IAPS and QUANTERALL)

Stoyan Mishev, Vesselin Gueorguiev and Vladimir Gerdjikov

IAPS INSTITUTE *for* ADVANCED PHYSICAL STUDIES

NEW BULGARIAN UNIVERSITY

December 16, 2022

Factor group and hidden subgroup problem

Discrete Logarithm as a Hidden Subgroup Problem

Factor group and hidden subgroup problem

Definition 6.15 Let $\mathcal{H}$ be a subgroup of the group $\mathcal{G}$ and let S be a finite set. We say that a function $f : \mathcal{G} \to S$ **hides the subgroup** $\mathcal{H}$ if for any $g_1, g_2 \in \mathcal{G}$

$$f(g_1) = f(g_2) \quad \Leftrightarrow \quad g_1^{-1} g_2 \in \mathcal{H}.$$

[1] A subgroup H of the group G is normal in G ($N \triangleleft G$) if and only if $gng^{-1} \in N$ for all $g \in G$ and $n \in N$. They can be used to construct quotient groups of the given group.

Factor group and hidden subgroup problem

Definition 6.15 Let $\mathcal{H}$ be a subgroup of the group $\mathcal{G}$ and let S be a finite set. We say that a function $f : \mathcal{G} \to S$ **hides the subgroup** $\mathcal{H}$ if for any $g_1, g_2 \in \mathcal{G}$

$$f(g_1) = f(g_2) \quad \Leftrightarrow \quad g_1^{-1} g_2 \in \mathcal{H}.$$

Exercise 6.73 Let $\mathcal{H}$ be a subgroup of the group $\mathcal{G}$ and $f : \mathcal{G} \to S$, where S is a finite set. Show that then

$$f \text{ hides } \mathcal{H} \quad \Leftrightarrow \quad \forall g_1, g_2 \in \mathcal{G} \quad f(g_1) = f(g_2) \Leftrightarrow g_1\mathcal{H} = g_2\mathcal{H}.$$

[1] A subgroup H of the group G is normal in G ($N \triangleleft G$) if and only if $gng^{-1} \in N$ for all $g \in G$ and $n \in N$. They can be used to construct quotient groups of the given group.

Factor group and hidden subgroup problem

Definition 6.15 Let $\mathcal{H}$ be a subgroup of the group $\mathcal{G}$ and let S be a finite set. We say that a function $f : \mathcal{G} \to S$ **hides the subgroup** $\mathcal{H}$ if for any $g_1, g_2 \in \mathcal{G}$

$$f(g_1) = f(g_2) \quad \Leftrightarrow \quad g_1^{-1} g_2 \in \mathcal{H}.$$

Exercise 6.73 Let $\mathcal{H}$ be a subgroup of the group $\mathcal{G}$ and $f : \mathcal{G} \to S$, where S is a finite set. Show that then

$$f \text{ hides } \mathcal{H} \quad \Leftrightarrow \quad \forall g_1, g_2 \in \mathcal{G} \quad f(g_1) = f(g_2) \Leftrightarrow g_1\mathcal{H} = g_2\mathcal{H}.$$

If f hides a normal subgroup H, then it can be seen as an injective function on the quotient group G/H.

[1] A subgroup H of the group G is normal in G ($N \triangleleft G$) if and only if $gng^{-1} \in N$ for all $g \in G$ and $n \in N$. They can be used to construct quotient groups of the given group.

Factor group and hidden subgroup problem

Definition 6.15 Let $\mathcal{H}$ be a subgroup of the group $\mathcal{G}$ and let S be a finite set. We say that a function $f : \mathcal{G} \to S$ **hides the subgroup** $\mathcal{H}$ if for any $g_1, g_2 \in \mathcal{G}$

$$f(g_1) = f(g_2) \quad \Leftrightarrow \quad g_1^{-1} g_2 \in \mathcal{H}.$$

Exercise 6.73 Let $\mathcal{H}$ be a subgroup of the group $\mathcal{G}$ and $f : \mathcal{G} \to S$, where S is a finite set. Show that then

$$f \text{ hides } \mathcal{H} \quad \Leftrightarrow \quad \forall g_1, g_2 \in \mathcal{G} \quad f(g_1) = f(g_2) \Leftrightarrow g_1\mathcal{H} = g_2\mathcal{H}.$$

If f hides a normal subgroup H, then it can be seen as an injective function on the quotient group G/H.[1]

[1] A subgroup H of the group G is normal in G ($N \triangleleft G$) if and only if $gng^{-1} \in N$ for all $g \in G$ and $n \in N$. They can be used to construct quotient groups of the given group.

Definition 6.16 Let f hide the subgroup $\mathcal{H}$ of the group $\mathcal{G}$. The problem to identify $\mathcal{H}$ with the help of f is called **Hidden Subgroup Problem (HSP)**.

In case $\mathcal{G}$ is a finite abelian group it is called the **Abelian Hidden Subgroup Problem (AHSP)**.

HSP is defined as the problem to identify H as efficiently as possible with the help of f , i.e. with as few evaluations of f as possible.

Definition 6.16 Let f hide the subgroup $\mathcal{H}$ of the group $\mathcal{G}$. The problem to identify $\mathcal{H}$ with the help of f is called **Hidden Subgroup Problem (HSP)**.

In case $\mathcal{G}$ is a finite abelian group it is called the **Abelian Hidden Subgroup Problem (AHSP)**.

HSP is defined as the problem to identify H as efficiently as possible with the help of f , i.e. with as few evaluations of f as possible.
If $|G|$ is the order of G then on a quantum computer we would need about $n := \log_2 |G|$ qubits to identify all elements of G - $\{|g_1\rangle, \ldots, |g_{|G|}\rangle\}$. If the group is Abelian then $\langle g_l | g_k \rangle = \delta_{lk}$. $|g_l\rangle \in H^A$

Definition 6.16 Let f hide the subgroup $\mathcal{H}$ of the group $\mathcal{G}$. The problem to identify $\mathcal{H}$ with the help of f is called **Hidden Subgroup Problem (HSP)**.

In case $\mathcal{G}$ is a finite abelian group it is called the **Abelian Hidden Subgroup Problem (AHSP)**.

HSP is defined as the problem to identify H as efficiently as possible with the help of f , i.e. with as few evaluations of f as possible.
If $|G|$ is the order of G then on a quantum computer we would need about $n := \log_2 |G|$ qubits to identify all elements of G - $\{|g_1\rangle, \ldots, |g_{|G|}\rangle\}$. If the group is Abelian then $\langle g_l | g_k \rangle = \delta_{lk}$. $|g_l\rangle \in H^A$
The set S (# of elements is $|S|$) is ordered and its elements s_j are labeled by j ($s_j \equiv j$). The corresponding vectors in the Hilbert space are $|j\rangle \in H^B$.

Steps to find the Abelian subgroup given f

STEP 1

$$|\Psi_0\rangle := \frac{1}{\sqrt{|\mathcal{G}|}} \sum_{g\in\mathcal{G}} |g\rangle^A \otimes |0\rangle^B \in \mathbb{H}^A \otimes \mathbb{H}^B .$$

STEP 2

AHSP Assumption 2 *For $f : \mathcal{G} \to S$ there exists an implementation of a unitary U_f defined by its action on the ONB*

$$\left\{ |g\rangle \otimes |y\rangle \,\middle|\, g \in \mathcal{G},\ 0 \le y < 2^m \right\} \subset \mathbb{H}^A \otimes \mathbb{H}^B \tag{6.92}$$

as

$$\begin{aligned} U_f : \mathbb{H}^A \otimes \mathbb{H}^B &\longrightarrow \mathbb{H}^A \otimes \mathbb{H}^B \\ |g\rangle \otimes |y\rangle &\longmapsto |g\rangle \otimes |y \boxplus \widetilde{f(g)}\rangle \end{aligned} , \tag{6.93}$$

and the number of computational steps S_2 for the application of U_f satisfies

$$\mathrm{S}_2(|\mathcal{G}|) \in \mathrm{poly}\left(\log_2(|\mathcal{G}|)\right) \quad \textit{for } |\mathcal{G}| \to \infty .$$

STEP 3

Construct

$$|\Psi_1\rangle := U_f|\Psi_0\rangle = \frac{1}{\sqrt{|\mathcal{G}|}}\sum_{g\in\mathcal{G}} U_f\big(|g\rangle\otimes|0\rangle\big)$$

$$\underbrace{=}_{(6.92)} \frac{1}{\sqrt{|\mathcal{G}|}}\sum_{g\in\mathcal{G}} |g\rangle\otimes|\widetilde{f(g)}\rangle \in \mathbb{H}^A\otimes\mathbb{H}^B$$

Steps to find the Abelian subgroup given f

STEP 3

Construct

$$|\Psi_1\rangle := U_f|\Psi_0\rangle = \frac{1}{\sqrt{|\mathcal{G}|}}\sum_{g\in\mathcal{G}} U_f\big(|g\rangle\otimes|0\rangle\big)$$

$$\underbrace{=}_{(6.92)} \frac{1}{\sqrt{|\mathcal{G}|}}\sum_{g\in\mathcal{G}} |g\rangle\otimes|\widetilde{f(g)}\rangle \in \mathbb{H}^A\otimes\mathbb{H}^B$$

STEP 4

Measure the qubits only in H^A

STEP 3

Construct

$$|\Psi_1\rangle := U_f|\Psi_0\rangle = \frac{1}{\sqrt{|\mathcal{G}|}}\sum_{g\in\mathcal{G}} U_f\big(|g\rangle\otimes|0\rangle\big)$$

$$\underbrace{=}_{(6.92)} \frac{1}{\sqrt{|\mathcal{G}|}}\sum_{g\in\mathcal{G}} |g\rangle\otimes|\widetilde{f(g)}\rangle \in \mathbb{H}^A\otimes\mathbb{H}^B$$

STEP 4

Measure the qubits only in H^A by the operator

$$\rho^A = \mathrm{tr}^B(\rho) = \mathrm{tr}^B(|\Psi_1\rangle\langle\Psi_1|) = \frac{|H|}{|G|}\sum_{[g]_H\in G/H} |\Psi^A_{[g]_H}\rangle\langle\Psi^A_{[g]_H}|$$

$$|\Psi^A_{[g]_H}\rangle := \frac{1}{\sqrt{|H|}}\sum_{k\in[g]_H} |k\rangle$$

STEP 5

Apply the Fourier transform

$$F_{\mathcal{G}} = \frac{1}{\sqrt{|\mathcal{G}|}} \sum_{g \in \mathcal{G}} \sum_{\chi \in \widehat{\mathcal{G}}} \chi(g) |\chi\rangle\langle g|$$

$$\rho^A \to F_G \rho^A F_G^*$$

$$F_{\mathcal{G}} \rho^A F_{\mathcal{G}}^* = \frac{|\mathcal{H}|}{|\mathcal{G}|} \sum_{[g]_{\mathcal{H}} \in \mathcal{G}/\mathcal{H}} \left(\sum_{\chi \in \mathcal{H}^\perp} \chi(g) |\chi\rangle \right) \left(\sum_{\xi \in \mathcal{H}^\perp} \overline{\xi(g)} \langle \xi| \right)$$

STEP 5

Apply the Fourier transform

$$F_{\mathcal{G}} = \frac{1}{\sqrt{|\mathcal{G}|}} \sum_{g \in \mathcal{G}} \sum_{\chi \in \widehat{\mathcal{G}}} \chi(g) |\chi\rangle\langle g|$$

$$\rho^A \to F_G \rho^A F_G^*$$

$$F_{\mathcal{G}} \rho^A F_{\mathcal{G}}^* = \frac{|\mathcal{H}|}{|\mathcal{G}|} \sum_{[g]_{\mathcal{H}} \in \mathcal{G}/\mathcal{H}} \left(\sum_{\chi \in \mathcal{H}^\perp} \chi(g) |\chi\rangle \right) \left(\sum_{\xi \in \mathcal{H}^\perp} \overline{\xi(g)} \langle \xi| \right)$$

STEP 6

Let $\zeta \in H_\perp$ and let $|\zeta\rangle$ be the corresponding basis in H^A with a projector on it $P_\zeta = |\zeta\rangle\langle\zeta|$. It turns out that the probability to detect the state $|\zeta\rangle$ when observing H^A prepared in the state $F_G \rho^A F_G^*$ equals 1.

STEP 5

Apply the Fourier transform

$$F_{\mathcal{G}} = \frac{1}{\sqrt{|\mathcal{G}|}} \sum_{g \in \mathcal{G}} \sum_{\chi \in \widehat{\mathcal{G}}} \chi(g) |\chi\rangle\langle g|$$

$$\rho^A \to F_G \rho^A F_G^*$$

$$F_{\mathcal{G}} \rho^A F_{\mathcal{G}}^* = \frac{|\mathcal{H}|}{|\mathcal{G}|} \sum_{[g]_{\mathcal{H}} \in \mathcal{G}/\mathcal{H}} \left(\sum_{\chi \in \mathcal{H}^\perp} \chi(g) |\chi\rangle \right) \left(\sum_{\xi \in \mathcal{H}^\perp} \overline{\xi(g)} \langle \xi| \right)$$

STEP 6

Let $\zeta \in H_\perp$ and let $|\zeta\rangle$ be the corresponding basis in H^A with a projector on it $P_\zeta = |\zeta\rangle\langle\zeta|$. It turns out that the probability to detect the state $|\zeta\rangle$ when observing H^A prepared in the state $F_G \rho^A F_G^*$ equals 1.

When observing the sub-system H^A after the Fourier transform we will always find a state $|\zeta\rangle$ that corresponds to a character $\zeta \in H_\perp$.

Discrete Logarithm as a Hidden Subgroup Problem

THANK YOU FOR YOUR ATTENTION!

БЛАГОДАРЯ ЗА ВНИМАНИЕТО!