Chapter 1

Quantum collision algorithms

1.1 Contact Information

If you have any questions about the course, contact me at andre.chailloux@inria.fr. My course can be found on my webpage: https://who.rocq.inria.fr/Andre.Chailloux/ (with ‘A’ and ‘C’ in capitals).

1.2 Cryptographic hash functions

A cryptographic hash function \( H : \{0,1\}^* \rightarrow \{0,1\}^n \) must satisfy the following properties.

- One-wayness: for a random \( y \in \{0,1\}^n \), it should be hard to find \( x \), such that \( H(x) = y \).
- Second-preimage resistance: for a fixed \( x \), it should be hard to find \( x' \neq x \) such that \( H(x) = H(x') \).
- Collision resistance: it should be hard to find \( x, x' \neq x \) such that \( H(x) = H(x') \).

Brute force complexity of those algorithms classically: One-wayness: \( O(2^n) \), second-preimage: \( O(2^n) \), collision resistance: \( O(2^{n/2}) \).

Quantum brute force complexity: One-wayness: \( O(2^{n/2}) \), second-preimage: \( O(2^{n/2}) \), collision resistance: \( ?? \).

Collision problem. Here, we fix the input space to be of \( n \) bits as well, and we consider a random function \( f \). We assume the function is efficiently computable and fix it’s computing time to 1.

<table>
<thead>
<tr>
<th>Collision problem</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input: a random function ( f : {0,1}^n \rightarrow {0,1}^n ).</td>
</tr>
<tr>
<td>Goal: find ((x,y)) such that ( f(x) = f(y) ) and ( x \neq y ). Because ( f ) is random, many such couples.</td>
</tr>
</tbody>
</table>

1.3 A classical algorithm

1. Pick a parameter \( r \). Pick a random subset \( I \subseteq \{0,1\}^n \) of size \( r \). Construct the list \( L = \{f(i)\}_{i \in I} \) and sort it. If we find 2 values \( i, j \in I \) such that \( f(i) = f(j) \) and \( i \neq j \), output \((i,j)\). Else:
2. Compute \( f(x) \) for random values \( x \notin I \) and for each such \( f(x) \), we test if \( f(x) \in L \). We continue until we find \( f(x) \in L \). Since \( f \) is random, each \( x \notin I \) will satisfy \( f(x) \in L \) with probability \( \frac{r}{2^n} \). We need to test on average \( O(\frac{2^n}{r}) \) to find one with high probability.

This algorithm uses the well known birthday paradox. The first step takes time \( O(r \log(r)) \) and the second one \( O(\frac{2^n \log(n)}{r}) \). By taking \( r = 2^{n/2} \), we have an algorithm running in time \( O(\text{poly}(n)2^{n/2}) \).

There are also algorithms that use a smaller amount of memory.

### 1.4 Quantum algorithms

#### 1.4.1 A naive way

Consider the function \( g(x, y) = 1 \) if \( (f(x) = f(y) \land x \neq y) \) and \( g(x, y) = 0 \) otherwise. We apply Grover on \( g \). Because \( f \) is random, there are on average \( O(2^n) \) couples \((x, y)\) such that \( g(x, y) = 1 \). We perform Grover on \( g \) which takes time \( O(\log^2 n) \). This is not significantly better than the classical algorithm.

#### 1.4.2 The quantum BHT (Brassard,Hoyer and Tapp) Algorithm

1. Pick a parameter \( r \). Pick a random subset \( I \subseteq \{0, 1\}^n \) of size \( r \). Construct the list \( L = \{ f(i) \}_{i \in I} \).
2. Let \( g : \{0, 1\}^n \rightarrow \{0, 1\} \) satisfying \( g(x) = 1 \iff [x \notin I \land \exists i \in I, f(x) = f(i)] \approx r \) solutions when \( r \ll 2^n \).
3. Apply Grover on \( g \). Find \( y \) such that \( g(y) = 1 \).
4. Find \( i \in I \) s.t. \( f(i) = f(y) \). Output \( (i, y) \).

#### Time analysis of BHT

- List creation: time \( r \log(r) \).
- Time to compute \( O_g \): classically, \( g \) takes time \( n \log(r) \). Can we use the standard reduction to construct \( O_g \) from \( g \)?
- Time to compute \( O_g \): \( n \log(r) \).
- Grover on \( g \). \( g \) is a function from \( \{0, 1\}^n \setminus I \rightarrow \{0, 1\} \). The input space is of size \( 2^n - r \) and there are on average \( r \) solutions. So we need to iterate Grover \( \approx \sqrt{\frac{2^n - r}{r}} \) to find a solution to \( g \). We define \( |\psi_i\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0, 1\}^n} |x\rangle |g(x)\rangle \)

\[
QTime(BHT) = \frac{r \log(r)}{\text{List L creation}} + \sqrt{\frac{2^n - r}{r}} \cdot \left( \frac{n \log(r)}{\text{nb. of Grover iterations}} + 1 \right).
\]
If we take \( r = \frac{2^{n/3}}{\text{Time}^{1/3}(f)} \), we obtain

\[
Q\text{Time}(BHT) = \tilde{O}(\text{Time}^{1/3}(f) \cdot 2^{n/3}).
\]

**On quantum RAM, and on how to compute \( O_g \).**

The classical algorithm to compute \( g \) has a sorted list \( L = (y_1, \ldots, y_r) \) that contains the values \( f(x) \) for \( x \in I \) and performs a dichotomic search on the memory.

If we have access to the elements in \( L \) in quantum registers \( |y_1\rangle, \ldots, |y_r\rangle \) as well as access to quantum RAM, then we can perform the membership oracle for \( L \) in time \( O(n \log(r)) \) via dichotomic search. The proof will be omitted here but the idea is that with RAM access, classical dichotomic search can be expressed as a classical circuit of size \( O(n \log(r)) \). Similarly as in the transformation.
from classical circuits to quantum circuits, we can create the quantum membership oracle from dichotomic search.

If we don’t have access to that QRAM, then the above can be done in time \( nr \) by checking each element separately. This is way worst for very large lists like in our example.

**Quantum collision protocols without QRAM and with small quantum memory.** Since 2016, we know that there exists a quantum algorithm that runs in time \( O(2^{2n/5}) \) that solves the collision problem with \( n \) qubits and no QRAM.

**Tightness of the algorithm.** The \( \tilde{O}(2^{n/3}) \) quantum algorithm is tight, meaning that there is a matching lower bound.

**Overview of known quantum algorithm for cryptography**

Here is an overview of quantum algorithms so far.

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Qtime</th>
<th>Qspace</th>
<th>Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shor (factoring)</td>
<td>poly(n)</td>
<td>( n )</td>
<td>RSA</td>
</tr>
<tr>
<td>Discrete log (elliptic curves)</td>
<td>poly(n)</td>
<td>( n )</td>
<td>Diffie Hellman, ECDH, ECDSA</td>
</tr>
<tr>
<td>Dihedral subgroup (solves SVP)</td>
<td>subexp(n)</td>
<td>( n )</td>
<td>NTRU, lattice based</td>
</tr>
<tr>
<td>Grover</td>
<td>( 2^{n/2} )</td>
<td>( n )</td>
<td>generic</td>
</tr>
<tr>
<td>Collision</td>
<td>( 2^{n/3} ) or ( 2^{2n/5} )</td>
<td>( 2^{n/3} ) or ( n )</td>
<td>generic</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(hash functions, symmetric)</td>
</tr>
</tbody>
</table>
Chapter 2

Lower bound for Grover’s algorithm

2.1 Lower bound for Grover’s algorithm and quantum complexity

Here, we show that for the search problem, Grover’s algorithm is essentially optimal so we cannot expect anything better than $2^{n/2}$.

Framework

- Input: function $f : \{0,1\}^n \rightarrow \{0,1\}$. Goal: find $x$ st. $f(x) = 1$.
- Access to $O_f(|x\rangle_X|b\rangle_B) = |x\rangle_X|b \oplus f(x)\rangle_B$.
- How many calls do I have to make to $O_f$ to find $x$ in the worst case?
- Result here: need $\Omega(2^{n/2})$ calls to $O_f$ to work wp. 1.

General structure of a $q$-query search algorithm

- Initialize:

$$|\psi^{0,f}\rangle = |\psi^0\rangle = \sum_{x \in \{0,1\}^n} \sum_{b \in \{0,1\}} \alpha^0_{x,b} |x\rangle_X|b\rangle_B|E_{x,b}\rangle_E$$

st. $\sum_{x,b} |\alpha^0_{x,b}|^2 = 1$
• 1 step: apply a unitary $O_f$ on XB and $U^{i+1}$ independent of $f$ on XBE.
\[
|\psi^{i+1,f}\rangle = U^{i+1}(O_f \otimes I_E)(|\psi^i,f\rangle)
\]
\[
= \sum_{x \in \{0,1\}^n} \sum_{b \in \{0,1\}} \alpha_{x,b}^{i+1,f} |x,b\rangle_{XB} |E_{x,b}^{i+1,f}\rangle_E
\]

Again, $\sum_{x,b} |\alpha_{x,b}^{i+1,f}|^2 = 1$.

• Final state: $|\psi^{q,f}\rangle$. Procedure to extract a solution from this state.

Main idea

• For any $y \in \{0,1\}^n$, we define $f_y$ satisfying $f_y(y) = 1$ and $f_y(x) = 0$ for $x \neq y$.

• Consider any $y,z \in \{0,1\}^n$. The search procedure should output $y$ when querying $f_y$ and $z$ when querying $f_z$.
\[
\Rightarrow |\psi^{q,f_y}\rangle \text{ and } |\psi^{q,f_z}\rangle \text{ are orthogonal.}
\]

• But $|\psi^{0,f_y}\rangle = |\psi^{0,f_z}\rangle$. Idea is to show that each query cannot separate those 2 states too much (on average on $y,z$).

The Euclidian norm on quantum states We consider the Euclidian $\| \cdot \|$. Recall that
\[
\| \sum_i \alpha_i |i\rangle \| = \sqrt{\sum_i |\alpha_i|^2}.
\]

For any 2 quantum states $|\phi_1\rangle, |\phi_2\rangle$ and any Unitary $U$, we have $\| |\phi_1\rangle - |\phi_2\rangle \| = \| U(|\phi_1\rangle) - U(|\phi_2\rangle) \|$. One can also check that if $|\phi_1\rangle \perp |\phi_2\rangle$ then $\| |\phi_1\rangle - |\phi_2\rangle \| = \sqrt{2}$. We use an intermediate function, the all 0 function denoted $f_0$. Notice that $O_{f_0} = I$. We first show

Lemma 1. $\frac{1}{2^n} \sum_y \| |\psi^{q,f_y}\rangle - |\psi^{q,f_{y_0}}\rangle \| \geq \sqrt{2} \cdot \frac{2^n-1}{2^n}$.

Proof. Let $y_0 \in \{0,1\}^n$ that minimizes $\| |\psi^{q,f_y}\rangle - |\psi^{q,f_{y_0}}\rangle \|$. We have
\[
\frac{1}{2^n-1} \sum_{y \neq y_0} \| |\psi^{q,f_y}\rangle - |\psi^{q,f_{y_0}}\rangle \| = \sqrt{2}.
\]

from the orthogonality of those states. Moreover, by triangle inequality, we have
\[
\frac{1}{2^n-1} \sum_{y \neq y_0} \| |\psi^{q,f_y}\rangle - |\psi^{q,f_{y_0}}\rangle \| \leq \frac{1}{2^n-1} \sum_{y \neq y_0} \| |\psi^{q,f_y}\rangle - |\psi^{q,f_{y_0}}\rangle \| + \frac{1}{2^n-1} \sum_{y \neq y_0} \| |\psi^{q,f_y}\rangle - |\psi^{q,f_{y_0}}\rangle \| \leq \frac{2}{2^n-1} \sum_{y \neq y_0} \| |\psi^{q,f_y}\rangle - |\psi^{q,f_{y_0}}\rangle \|
\]

From there, we get the result:
\[
\frac{1}{2^n} \sum_y \| |\psi^{q,f_y}\rangle - |\psi^{q,f_{y_0}}\rangle \| \geq \frac{1}{2^n} \sum_{y \neq y_0} \| |\psi^{q,f_y}\rangle - |\psi^{q,f_{y_0}}\rangle \| \geq \frac{1}{\sqrt{2}} \cdot \frac{2^n-1}{2^n}.
\]

\[\square\]
So now, our goal is to bound this quantity as a function of $q$. This will give us the desired lower bound on $q$. We first prove the following:

**Lemma 2.** For any $i \in [0, q - 1]$, for any $y \in \{0, 1\}^n$, we have
\[
\left\| \psi^{i+1,f_y} - \psi^{i+1,f_y} \right\| \leq \left\| \psi^{i,f_y} - (O_{f_y} \otimes I)\psi^{i,f_y} \right\| + \left\| \psi^{i,f_y} - \psi^{i,f_y} \right\|.
\]

**Proof.** We have
\[
\left\| \psi^{i+1,f_y} - \psi^{i+1,f_y} \right\| = \left\| U^{i+1}\psi^{i,f_y} - U^{i+1}(O_{f_y} \otimes I)\psi^{i,f_y} \right\|
\leq \left\| U^{i+1}\psi^{i,f_y} - U^{i+1}(O_{f_y} \otimes I)\psi^{i,f_y} \right\| + \\
\left\| U^{i+1}(O_{f_y} \otimes I)\psi^{i,f_y} - U^{i+1}(O_{f_y} \otimes I)\psi^{i,f_y} \right\|
= \left\| \psi^{i,f_y} - (O_{f_y} \otimes I)\psi^{i,f_y} \right\| + \left\| \psi^{i,f_y} - \psi^{i,f_y} \right\|.
\]

We now prove our main proposition

**Proposition 1.**
\[
\frac{1}{2^n} \sum_y \left\| \psi^{q,f_y} - \psi^{q,f_y} \right\| \leq \frac{2q}{2^{n/2}}.
\]

**Proof.** Fix $i$ and $y$. We write
\[
\psi^{i,f_y} = \sum_{x \in \{0,1\}^n} \sum_{b \in \{0,1\}} \alpha^i_{x,b} |x,b\rangle_{XB} |E^i_{x,b}\rangle_E
\]
From the definition of $O_{f_y}$, we also have
\[
(O_{f_y} \otimes I)\psi^{i,f_y} = \sum_{x \neq y \in \{0,1\}^n} \sum_{b \in \{0,1\}} \alpha^i_{x,b} |x,b\rangle_{XB} |E^i_{x,b}\rangle_E + \sum_{b \in \{0,1\}} \alpha^i_{y,b} |y,b\rangle_{XB} |E^i_{y,b}\rangle_E
\]
for some unknown amplitudes $\alpha^i_{x,b}$ (the superscripts $f_y$ are omitted). For each $y, i$, this gives
\[
\left\| \psi^{i,f_y} - (O_{f_y} \otimes I)\psi^{i,f_y} \right\| = \sqrt{\sum_{x \neq y \in \{0,1\}^n} \sum_{b \in \{0,1\}} |\alpha^i_{x,b} - \alpha^i_{x,b}|^2 + \sum_{b \in \{0,1\}} \sum_{x \neq y \in \{0,1\}^n} |\alpha^i_{y,b} - \alpha^i_{y,b}|^2}
\leq \sqrt{2|\alpha^i_{y,0}|^2 + 2|\alpha^i_{y,1}|^2 + 2|\alpha^i_{y,0}|^2 + 2|\alpha^i_{y,1}|^2}
\leq 2\sqrt{|\alpha^i_{y,0}|^2 + |\alpha^i_{y,1}|^2}
\]
where the first inequality uses $|a - b|^2 \leq 2|a|^2 + 2|b|^2$ for any $a, b \in \mathbb{C}$. Plugging this into the inequality of Lemma 2 and performing a recursion, we get
\[
\left\| \psi^{q,f_y} - \psi^{q,f_y} \right\| \leq \sum_{i=0}^{q-1} 2\sqrt{|\alpha^i_{y,0}|^2 + |\alpha^i_{y,1}|^2}
\]
We average this over all $y$ and get.

$$
\frac{1}{2^n} \sum_y \left| \left| \psi^q f_0 \right| \right| \leq \frac{1}{2^n} \sum_{y \in \{0,1\}^n} \sum_{i=0}^{q-1} 2 \sqrt{|\alpha_{y,0}^i|^2 + |\alpha_{y,1}^i|^2}
$$

$$
\leq \frac{1}{2^{n/2}} \sum_{i=0}^{q-1} 2 \sqrt{\sum_y |\alpha_{y,0}^i|^2 + |\alpha_{y,1}^i|^2}
$$

$$
\leq \frac{2q}{2^{n/2}}.
$$

Using Lemma 4, we immediately have $q \geq \Omega(2^{n/2})$. \qed