

# Grover algorithm and Application

---

Pierre-Alain Fouque

Centre Inria of Université de Rennes

1. Grover Algorithm
2. Applications to Cryptanalysis

# Grover Algorithm

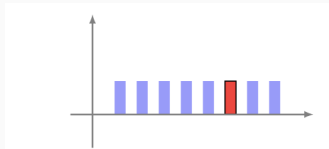
---

## Searching in a list of $N$ items

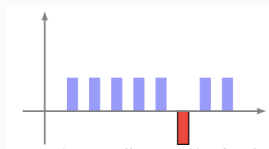
1. Sorted list:  $O(\log_2(N))$
2. Unsorted list:  $O(N)$
3. Grover (quantum):  $O(\sqrt{N})$ , but probabilistic algorithm

# Idea of the algorithm

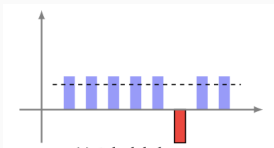
**Figure 1:** 3-qubit coefficients



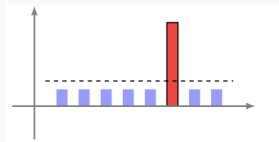
**Figure 2:** Negate one Coefficient



**Figure 3:** Mean Computation

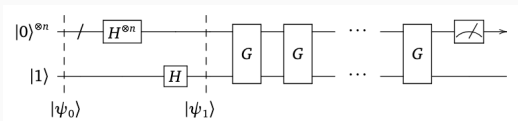


**Figure 4:** Symmetry wrt. the mean



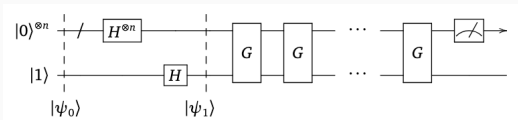
**Circuit:**  $f : \mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z}$  with  $f(k_0) = 1$  and  $f(k) = 0$  if  $k \neq k_0$

**Figure 5:** Grover Algorithm



**Circuit:**  $f : \mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z}$  with  $f(k_0) = 1$  and  $f(k) = 0$  if  $k \neq k_0$

**Figure 5:** Grover Algorithm



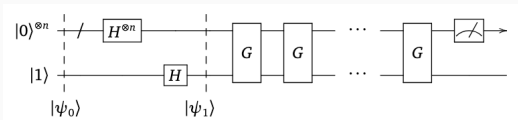
with

**Figure 6:** Grover Circuit



**Circuit:**  $f : \mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{Z}/2\mathbb{Z}$  with  $f(k_0) = 1$  and  $f(k) = 0$  if  $k \neq k_0$

**Figure 5:** Grover Algorithm



with

**Figure 6:** Grover Circuit



**Proposition:**

The measure outputs the correct index  $k_0$  with probability  $\geq 1 - \frac{4}{N}$ , if we use  $\approx \frac{\pi}{4} \sqrt{N}$  gates with complexity  $O(\sqrt{N})$

# Application of Grover Transformation

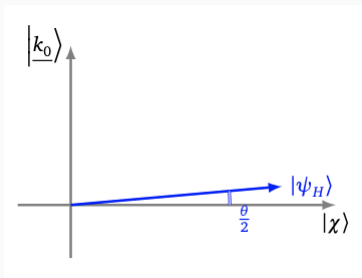
## Geometric interpretation

- $|\psi_H\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |\underline{k}\rangle = \sqrt{\frac{N-1}{N}} |\chi\rangle + \frac{1}{\sqrt{N}} |\underline{k}_0\rangle$

# Application of Grover Transformation

## Geometric interpretation

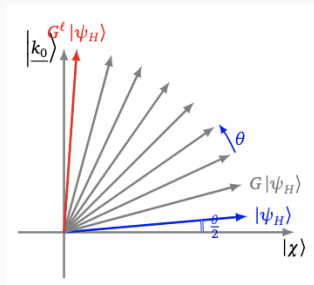
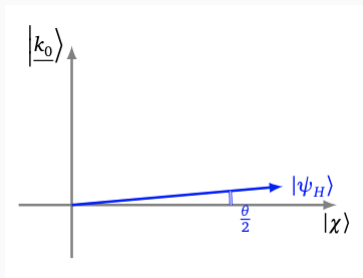
- $|\psi_H\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |\underline{k}\rangle = \sqrt{\frac{N-1}{N}} |\chi\rangle + \frac{1}{\sqrt{N}} |\underline{k}_0\rangle$
- $|\psi_H\rangle = \cos\left(\frac{\theta}{2}\right) |\chi\rangle + \sin\left(\frac{\theta}{2}\right) |\underline{k}_0\rangle$ ,  $\frac{\theta}{2} = \langle |\chi\rangle, |\psi_H\rangle \rangle$  and  $\sin\left(\frac{\theta}{2}\right) = \frac{1}{\sqrt{N}}$



# Application of Grover Transformation

## Geometric interpretation

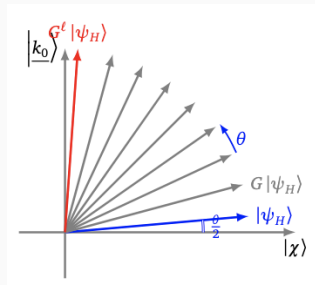
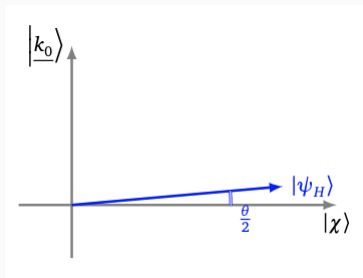
- $|\psi_H\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle = \sqrt{\frac{N-1}{N}} |\chi\rangle + \frac{1}{\sqrt{N}} |k_0\rangle$
- $|\psi_H\rangle = \cos\left(\frac{\theta}{2}\right) |\chi\rangle + \sin\left(\frac{\theta}{2}\right) |k_0\rangle$ ,  $\frac{\theta}{2} = \langle |\chi\rangle, |\psi_H\rangle \rangle$  and  $\sin\left(\frac{\theta}{2}\right) = \frac{1}{\sqrt{N}}$



# Application of Grover Transformation

## Geometric interpretation

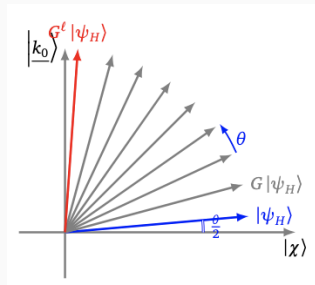
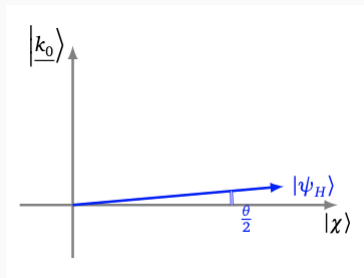
- $|\psi_H\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle = \sqrt{\frac{N-1}{N}} |\chi\rangle + \frac{1}{\sqrt{N}} |k_0\rangle$
- $|\psi_H\rangle = \cos(\frac{\theta}{2}) |\chi\rangle + \sin(\frac{\theta}{2}) |k_0\rangle$ ,  $\frac{\theta}{2} = \langle |\chi\rangle, |\psi_H\rangle \rangle$  and  $\sin(\frac{\theta}{2}) = \frac{1}{\sqrt{N}}$
- $G^\ell |\psi_H\rangle = \cos(\theta_\ell) |\chi\rangle + \sin(\theta_\ell) |k_0\rangle$



# Application of Grover Transformation

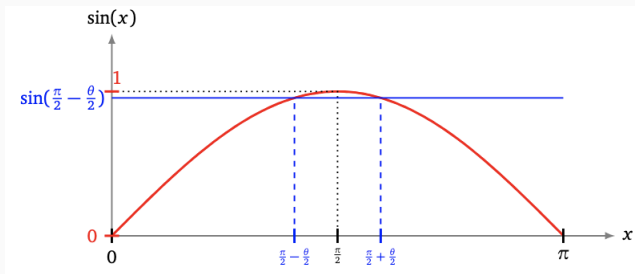
## Geometric interpretation

- $|\psi_H\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle = \sqrt{\frac{N-1}{N}} |\chi\rangle + \frac{1}{\sqrt{N}} |k_0\rangle$
- $|\psi_H\rangle = \cos\left(\frac{\theta}{2}\right) |\chi\rangle + \sin\left(\frac{\theta}{2}\right) |k_0\rangle$ ,  $\frac{\theta}{2} = \langle |\chi\rangle, |\psi_H\rangle \rangle$  and  $\sin\left(\frac{\theta}{2}\right) = \frac{1}{\sqrt{N}}$
- $G^\ell |\psi_H\rangle = \cos(\theta_\ell) |\chi\rangle + \sin(\theta_\ell) |k_0\rangle$
- As  $\sin\left(\frac{\theta}{2}\right) = \frac{1}{\sqrt{N}}$ ,  $\frac{\theta}{2} \approx \frac{1}{\sqrt{N}}$ , and  $\ell\theta \approx \frac{\pi}{2}$ , so  $\ell \approx \frac{\pi}{2\theta}$ , and  $\ell \approx \frac{\pi}{4} \sqrt{N}$



Probability  $p = |\sin(\theta_\ell)|^2$ , where  $\theta_\ell = \frac{\theta}{2} + \ell\theta$

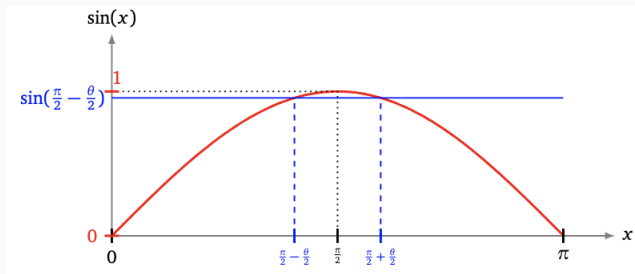
$\frac{\pi}{2} - \frac{\theta}{2} < \theta_\ell \leq \frac{\pi}{2} + \frac{\theta}{2}$  as  $\ell\theta$  multiple of  $\theta$  closest to  $\frac{\pi}{2}$



Probability  $p = |\sin(\theta_\ell)|^2$ , where  $\theta_\ell = \frac{\theta}{2} + \ell\theta$

$\frac{\pi}{2} - \frac{\theta}{2} < \theta_\ell \leq \frac{\pi}{2} + \frac{\theta}{2}$  as  $\ell\theta$  multiple of  $\theta$  closest to  $\frac{\pi}{2}$

1.  $\sin(\theta_\ell) \geq \sin(\frac{\pi}{2} - \frac{\theta}{2}) = \cos(\frac{\theta}{2}) \geq 1 - \frac{1}{2}(\frac{\theta}{2})^2$



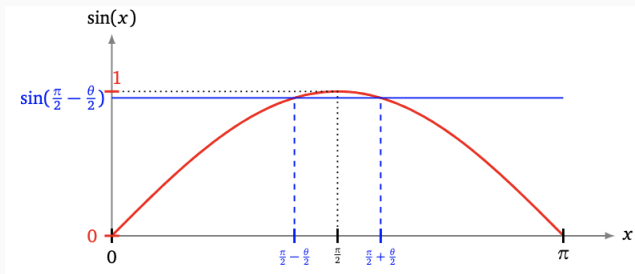
Probability  $p = |\sin(\theta_\ell)|^2$ , where  $\theta_\ell = \frac{\theta}{2} + \ell\theta$

$\frac{\pi}{2} - \frac{\theta}{2} < \theta_\ell \leq \frac{\pi}{2} + \frac{\theta}{2}$  as  $\ell\theta$  multiple of  $\theta$  closest to  $\frac{\pi}{2}$

1.  $\sin(\theta_\ell) \geq \sin(\frac{\pi}{2} - \frac{\theta}{2}) = \cos(\frac{\theta}{2}) \geq 1 - \frac{1}{2}(\frac{\theta}{2})^2$

2. As  $\sin(x) \geq \frac{x}{2}$  and  $\sin(\frac{\theta}{2}) = \frac{1}{\sqrt{N}}$ , then  $\frac{1}{\sqrt{N}} \geq \frac{\theta}{4}$ , and  $\frac{4}{N} \geq (\frac{\theta}{2})^2$ ,

$$\sin(\theta_\ell) \geq 1 - \frac{1}{2} \left(\frac{\theta}{2}\right)^2 \geq 1 - \frac{2}{N}.$$



**Probability  $p = |\sin(\theta_\ell)|^2$ , where  $\theta_\ell = \frac{\theta}{2} + \ell\theta$**

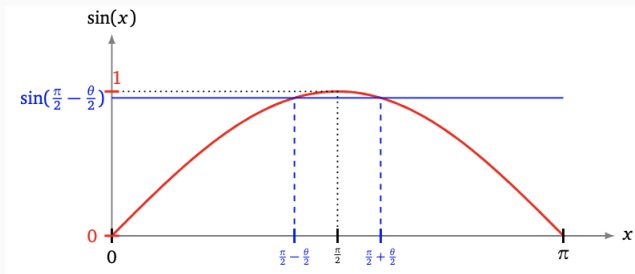
$\frac{\pi}{2} - \frac{\theta}{2} < \theta_\ell \leq \frac{\pi}{2} + \frac{\theta}{2}$  as  $\ell\theta$  multiple of  $\theta$  closest to  $\frac{\pi}{2}$

1.  $\sin(\theta_\ell) \geq \sin(\frac{\pi}{2} - \frac{\theta}{2}) = \cos(\frac{\theta}{2}) \geq 1 - \frac{1}{2}(\frac{\theta}{2})^2$

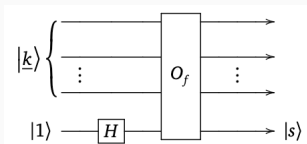
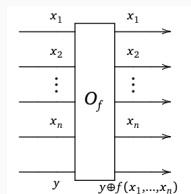
2. As  $\sin(x) \geq \frac{x}{2}$  and  $\sin(\frac{\theta}{2}) = \frac{1}{\sqrt{N}}$ , then  $\frac{1}{\sqrt{N}} \geq \frac{\theta}{4}$ , and  $\frac{4}{N} \geq (\frac{\theta}{2})^2$ ,

$$\sin(\theta_\ell) \geq 1 - \frac{1}{2} \left( \frac{\theta}{2} \right)^2 \geq 1 - \frac{2}{N}.$$

3.  $p = |\sin(\theta_\ell)|^2 \geq (1 - \frac{2}{N})^2 \geq 1 - \frac{4}{N}$  since  $(1 - x)^2 \geq 1 - 2x$



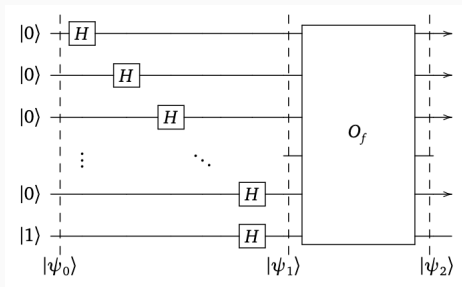
# Oracle Effect



**What happens for  $f(k_0) = 1$  and  $f(k) = 0$  for  $k \neq k_0$  ?**

- input of the last qubit:  $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
- $|s\rangle = (-1)^{f(k)} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \begin{cases} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) & \text{if } k \neq k_0 \\ -\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) & \text{if } k = k_0 \end{cases}$
- If the input is  $(|0\rangle + |\underline{1}\rangle + \dots + |\underline{k_0}\rangle + \dots + |\underline{2^n - 1}\rangle) \cdot (|0\rangle - |1\rangle)$ , the output is  $(|0\rangle + |\underline{1}\rangle + \dots - |\underline{k_0}\rangle + \dots + |\underline{2^n - 1}\rangle) \cdot (|0\rangle - |1\rangle)$

# Grover Circuit (Starting)



**Input qubit:**  $|\psi_0\rangle = |0 \dots 0\rangle \cdot |1\rangle = |\underline{0}\rangle \cdot |1\rangle$

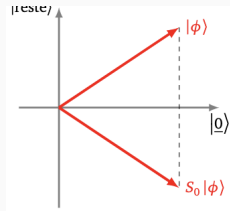
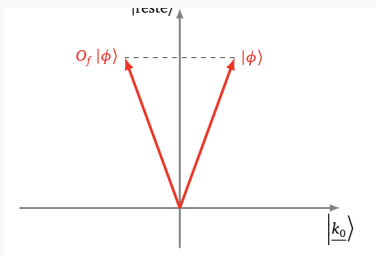
- Hadamard on the  $n$  first qubits:  $|\underline{0}\rangle + |\underline{1}\rangle + \dots + |\underline{k_0}\rangle + \dots + |\underline{2^n - 1}\rangle$   
and  $|\psi_1\rangle = H^{\otimes n} |\underline{0}\rangle \cdot H |1\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |\underline{k}\rangle \cdot \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$

- Oracle makes a sign “-” on  $k_0$ :

$$|\psi_2\rangle = O_f |\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} (-1)^{f(k)} |\underline{k}\rangle \cdot \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} (|\underline{0}\rangle + |\underline{1}\rangle + \dots - |\underline{k_0}\rangle + \dots + |\underline{2^n - 1}\rangle) \cdot \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

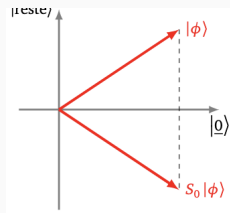
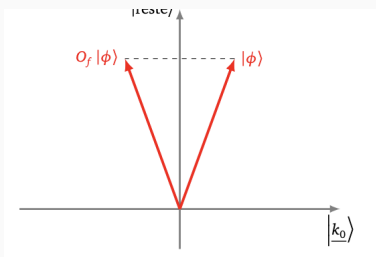
# Geometric Transform



**Input  $n$ -qubit**  $|\phi\rangle = \alpha |k_0\rangle + \sum_{k \neq k_0} \alpha_k |k\rangle$

- Oracle:  $O_f |\phi\rangle = -\alpha |k_0\rangle + \sum_{k \neq k_0} \alpha_k |k\rangle$
- Symmetry w.r.t.  $(2^n - 1)$ -hyperplane containing all other directions

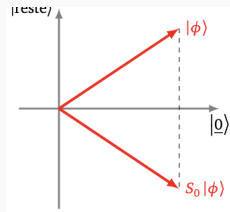
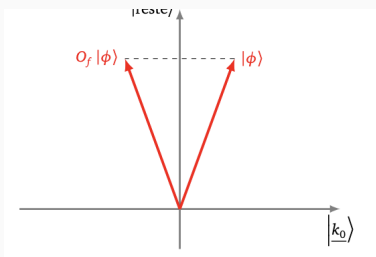
# Geometric Transform



**Input  $n$ -qubit**  $|\phi\rangle = \alpha |k_0\rangle + \sum_{k \neq k_0} \alpha_k |k\rangle$

- Oracle:  $O_f |\phi\rangle = -\alpha |k_0\rangle + \sum_{k \neq k_0} \alpha_k |k\rangle$
- Symmetry w.r.t.  $(2^n - 1)$ -hyperplane containing all other directions
- Assume,  $S_0$  is the symmetry of axis  $|0\rangle$ :  $S_0 = 2|0\rangle\langle 0| - I$ .
- Check  $S_0 |0\rangle = |0\rangle$  and  $S_0 |\phi\rangle = -|\phi\rangle$  if  $\langle 0|\phi\rangle$ . Matrix? Unitary?

# Geometric Transform

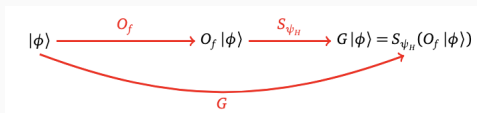


**Input  $n$ -qubit**  $|\phi\rangle = \alpha |k_0\rangle + \sum_{k \neq k_0} \alpha_k |k\rangle$

- Oracle:  $O_f |\phi\rangle = -\alpha |k_0\rangle + \sum_{k \neq k_0} \alpha_k |k\rangle$
- Symmetry w.r.t.  $(2^n - 1)$ -hyperplane containing all other directions
- Assume,  $S_0$  is the symmetry of axis  $|0\rangle$ :  $S_0 = 2|0\rangle\langle 0| - I$ .
- Check  $S_0 |0\rangle = |0\rangle$  and  $S_0 |\phi\rangle = -|\phi\rangle$  if  $\langle 0|\phi\rangle$ . Matrix? Unitary?
- More generally,  $S_{\psi_H}$  symmetry axis  $|\psi_H\rangle = H^{\otimes n} |0\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle$
- $S_{\psi_H} = H^{\otimes n} \cdot S_0 \cdot H^{\otimes n}$

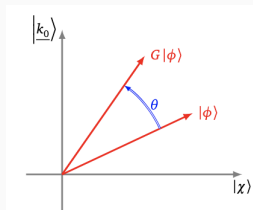
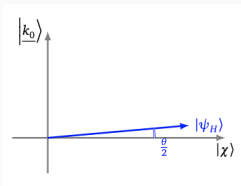
# Grover Transformation

Figure 7:  $G = S_{\psi_H} \circ O_f$



$$|\psi_H\rangle = \sqrt{\frac{N-1}{N}} |\chi\rangle + \frac{1}{\sqrt{N}} |\underline{k_0}\rangle$$

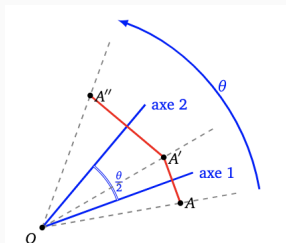
- Trigonometry:  $|\psi_H\rangle = \cos(\frac{\theta}{2}) |\chi\rangle + \sin(\frac{\theta}{2}) |\underline{k_0}\rangle$
- $\theta/2$ : angle  $\langle |\chi\rangle, |\psi_H\rangle \rangle$  and  $\cos(\frac{\theta}{2}) = \sqrt{\frac{N-1}{N}}$
- Grover Transformation is a rotation of angle  $\theta$



# Composition of two axial symmetries is a rotation

$G$  is the composition of two axial symmetries


- Symmetry  $O_f$  of axis  $|\chi\rangle$
- Symmetry  $S_{\psi_H}$  of axis  $|\psi_H\rangle$
- Angle between  $|\chi\rangle$  and  $|\psi_H\rangle$  is  $\theta/2$
- Consequently,  $G = S_{\psi_H} \circ O_f$  is the rotation of angle  $\theta$






$$\begin{cases} |0\rangle \mapsto |0\rangle \\ |1\rangle \mapsto -|1\rangle \end{cases}$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$




A quantum circuit diagram showing a single qubit line with a square gate labeled 'Z'.


$$\begin{cases} |0\rangle \mapsto |0\rangle \\ |1\rangle \mapsto -|1\rangle \end{cases} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

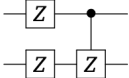


A quantum circuit diagram showing two qubit lines. The top line has a control dot connected to a square gate labeled 'Z' on the bottom line.

$$\begin{cases} |0.0\rangle \mapsto |0.0\rangle \\ |0.1\rangle \mapsto |0.1\rangle \\ |1.0\rangle \mapsto |1.0\rangle \\ |1.1\rangle \mapsto -|1.1\rangle \end{cases} \quad CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$


$$\begin{cases} |0\rangle \mapsto |0\rangle \\ |1\rangle \mapsto -|1\rangle \end{cases} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$


$$\begin{cases} |0.0\rangle \mapsto |0.0\rangle \\ |0.1\rangle \mapsto |0.1\rangle \\ |1.0\rangle \mapsto |1.0\rangle \\ |1.1\rangle \mapsto -|1.1\rangle \end{cases} \quad CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$


$$\begin{cases} |0.0\rangle \mapsto |0.0\rangle \\ |0.1\rangle \mapsto -|0.1\rangle \\ |1.0\rangle \mapsto -|1.0\rangle \\ |1.1\rangle \mapsto -|1.1\rangle \end{cases} \quad S_0 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

# $S_{\psi_H}$ Circuit

$$\text{---} \boxed{Z} \text{---} \quad \begin{cases} |0\rangle \mapsto |0\rangle \\ |1\rangle \mapsto -|1\rangle \end{cases} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\begin{array}{c} \bullet \\ | \\ \text{---} \\ | \\ \boxed{Z} \\ | \\ \text{---} \end{array} \quad \begin{cases} |0.0\rangle \mapsto |0.0\rangle \\ |0.1\rangle \mapsto |0.1\rangle \\ |1.0\rangle \mapsto |1.0\rangle \\ |1.1\rangle \mapsto -|1.1\rangle \end{cases} \quad CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

$$\begin{array}{c} \boxed{Z} \text{---} \bullet \\ | \\ \text{---} \\ | \\ \boxed{Z} \text{---} \boxed{Z} \\ | \\ \text{---} \end{array} \quad \begin{cases} |0.0\rangle \mapsto |0.0\rangle \\ |0.1\rangle \mapsto -|0.1\rangle \\ |1.0\rangle \mapsto -|1.0\rangle \\ |1.1\rangle \mapsto -|1.1\rangle \end{cases} \quad S_0 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

$$\text{---} \boxed{S_{\psi_H}} \text{---} = \text{---} \boxed{H} \text{---} \boxed{Z} \text{---} \bullet \text{---} \boxed{H} \text{---} \\ \text{---} \boxed{H} \text{---} \boxed{Z} \text{---} \boxed{Z} \text{---} \boxed{H} \text{---}$$

# Applications to Cryptanalysis

---

**Blockcipher**  $E : \{0, 1\}^n \times \{0, 1\}^\kappa \rightarrow \{0, 1\}^n$

- $k_0$  the secret key of a blockcipher and  $n \geq \kappa$
- Adversary can query  $x$  and obtain  $E(x, k_0)$  for any  $x$  of his choice
- Recover  $k_0$  or decrypt  $y$ . Brute force:  $O(2^\kappa)$  by trying all  $k$

# Application to Key Recovery

**Blockcipher**  $E : \{0, 1\}^n \times \{0, 1\}^\kappa \rightarrow \{0, 1\}^n$

- $k_0$  the secret key of a blockcipher and  $n \geq \kappa$
- Adversary can query  $x$  and obtain  $E(x, k_0)$  for any  $x$  of his choice
- Recover  $k_0$  or decrypt  $y$ . Brute force:  $O(2^\kappa)$  by trying all  $k$
- $f : \{0, 1\}^\kappa \rightarrow \{0, 1\}$  where  $f(k_0) = 1$  if  $E(x, k_0) \stackrel{?}{=} y$  else  $f(k) = 0$

# Application to Key Recovery

**Blockcipher**  $E : \{0, 1\}^n \times \{0, 1\}^\kappa \rightarrow \{0, 1\}^n$

- $k_0$  the secret key of a blockcipher and  $n \geq \kappa$
- Adversary can query  $x$  and obtain  $E(x, k_0)$  for any  $x$  of his choice
- Recover  $k_0$  or decrypt  $y$ . Brute force:  $O(2^\kappa)$  by trying all  $k$
- $f : \{0, 1\}^\kappa \rightarrow \{0, 1\}$  where  $f(k_0) = 1$  if  $E(x, k_0) \stackrel{?}{=} y$  else  $f(k) = 0$
- For a security level of  $\kappa$ ,  $\kappa$  (classically),  $2\kappa$  (quantumly)

# Application to hashing (I)

$H : \{0, 1\}^m \rightarrow \{0, 1\}^n$  with  $m > n$ : compressing function

**Preimage attack:** Given  $y$ , find  $x \in \{0, 1\}^n$  s.t.  $H(x) = y$   
Grover's algorithm find it in time  $2^{n/2}$

# Application to hashing (I)

$H : \{0, 1\}^m \rightarrow \{0, 1\}^n$  with  $m > n$ : compressing function

**Preimage attack:** Given  $y$ , find  $x \in \{0, 1\}^n$  s.t.  $H(x) = y$   
Grover's algorithm find it in time  $2^{n/2}$

## Improved cryptanalysis of collision search

1. According to the birthday paradox, randomly choosing  $N$  inputs  $x \in \{0, 1\}^m$ , if  $N \approx \sqrt{2^n}$ , constant probability of finding a collision

# Application to hashing (I)

$H : \{0, 1\}^m \rightarrow \{0, 1\}^n$  with  $m > n$ : compressing function

**Preimage attack:** Given  $y$ , find  $x \in \{0, 1\}^n$  s.t.  $H(x) = y$   
Grover's algorithm find it in time  $2^{n/2}$

## Improved cryptanalysis of collision search

1. According to the birthday paradox, randomly choosing  $N$  inputs  $x \in \{0, 1\}^m$ , if  $N \approx \sqrt{2^n}$ , constant probability of finding a collision
2. Let  $C, D \subset \{0, 1\}^m$  s.t.  $C \cap D = \emptyset$  and  $|C| = \ell$ ,  $|D| = \ell^2$
3. E.g.  $C = 0^{m-\log \ell} \cdot \{0, 1\}^{\log \ell}$  and  $D = 1^{m-2 \log \ell} \cdot \{0, 1\}^{2 \log \ell}$

# Application to hashing (I)

$H : \{0, 1\}^m \rightarrow \{0, 1\}^n$  with  $m > n$ : compressing function

**Preimage attack:** Given  $y$ , find  $x \in \{0, 1\}^n$  s.t.  $H(x) = y$

Grover's algorithm find it in time  $2^{n/2}$

## Improved cryptanalysis of collision search

1. According to the birthday paradox, randomly choosing  $N$  inputs  $x \in \{0, 1\}^m$ , if  $N \approx \sqrt{2^n}$ , constant probability of finding a collision
2. Let  $C, D \subset \{0, 1\}^m$  s.t.  $C \cap D = \emptyset$  and  $|C| = \ell$ ,  $|D| = \ell^2$
3. E.g.  $C = 0^{m-\log \ell} \cdot \{0, 1\}^{\log \ell}$  and  $D = 1^{m-2\log \ell} \cdot \{0, 1\}^{2\log \ell}$
4.  $C' = \{y_i : y_i = H(x_i) \text{ for all } x_i \in C\}$  and if  $y_i = y_j$  for  $i \neq j$ , a collision has been found

## Improved cryptanalysis of collision search

1.  $f : D \rightarrow \{0, 1\}$  s.t.  $f(x) = 1$  iff  $H(x) \in C'$  ( $f(x) = 1 \equiv$  collision)
2. Find  $x$  requires  $O(\sqrt{|D|})$  evaluations of  $f$  (or  $H$ ). Complexity:  
 $O(\ell + \sqrt{\ell^2}) = O(\ell)$

## Improved cryptanalysis of collision search

1.  $f : D \rightarrow \{0, 1\}$  s.t.  $f(x) = 1$  iff  $H(x) \in C'$  ( $f(x) = 1 \equiv$  collision)
2. Find  $x$  requires  $O(\sqrt{|D|})$  evaluations of  $f$  (or  $H$ ). Complexity:  
 $O(\ell + \sqrt{\ell^2}) = O(\ell)$
3. All values in  $C'$  are distinct, so if  $x \in D$ ,  $\Pr[H(x) \in C'] = \frac{\ell}{2^n}$
4.  $\Pr[x \in D' : H(x) \in C'] = 1 - \left(1 - \frac{\ell}{2^n}\right)^{\ell^2} \geq 1 - e^{\ell^3/2^n}$

## Improved cryptanalysis of collision search

1.  $f : D \rightarrow \{0, 1\}$  s.t.  $f(x) = 1$  iff  $H(x) \in C'$  ( $f(x) = 1 \equiv$  collision)
2. Find  $x$  requires  $O(\sqrt{|D|})$  evaluations of  $f$  (or  $H$ ). Complexity:  
 $O(\ell + \sqrt{\ell^2}) = O(\ell)$
3. All values in  $C'$  are distinct, so if  $x \in D$ ,  $\Pr[H(x) \in C'] = \frac{\ell}{2^n}$
4.  $\Pr[x \in D' : H(x) \in C'] = 1 - \left(1 - \frac{\ell}{2^n}\right)^{\ell^2} \geq 1 - e^{\ell^3/2^n}$
5. With  $\ell = \Theta(2^{n/3})$ , there is a constant probability of collision with  $\Theta(2^{n/3})$  evaluations of  $H$
6. For a security level of  $\kappa$ ,  $n = 2\kappa$  (classically),  $n = 3\kappa$  (quantumly)

# Post-Quantum Cryptography

---

## Motivations

- One of the most attractive alternatives among code-based, multivariate, isogenies...

## Motivations

- One of the most attractive alternatives among code-based, multivariate, isogenies...
- 3 standards already use hard problems on lattices

## Motivations

- One of the most attractive alternatives among code-based, multivariate, isogenies...
- 3 standards already use hard problems on lattices
- Very simple objects with very hard problems

## Motivations

- One of the most attractive alternatives among code-based, multivariate, isogenies...
- 3 standards already use hard problems on lattices
- Very simple objects with very hard problems
- Even approximation problems are hard: we do not know how to approximate them except with exponential factor in the dimension

## Motivations

- One of the most attractive alternatives among code-based, multivariate, isogenies...
- 3 standards already use hard problems on lattices
- Very simple objects with very hard problems
- Even approximation problems are hard: we do not know how to approximate them except with exponential factor in the dimension
- Well-studied mathematical object, in dimension 2 all problems are easy to solve ...

## Motivations

- One of the most attractive alternatives among code-based, multivariate, isogenies...
- 3 standards already use hard problems on lattices
- Very simple objects with very hard problems
- Even approximation problems are hard: we do not know how to approximate them except with exponential factor in the dimension
- Well-studied mathematical object, in dimension 2 all problems are easy to solve ...
- but in higher dimension, they are more difficult to solve

## Motivations

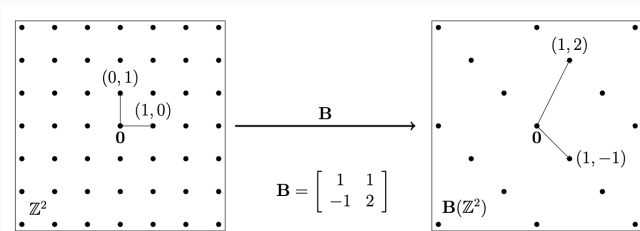
- One of the most attractive alternatives among code-based, multivariate, isogenies...
- 3 standards already use hard problems on lattices
- Very simple objects with very hard problems
- Even approximation problems are hard: we do not know how to approximate them except with exponential factor in the dimension
- Well-studied mathematical object, in dimension 2 all problems are easy to solve ...
- but in higher dimension, they are more difficult to solve
- Structured lattices come from number theory ideals or modules in cyclotomic number fields

**Definition:** studied by Lagrange, Gauss, Hermite, Minkowski in 18..

- A lattice is an infinite number of points in a Euclidean space:

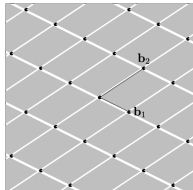
$$\mathbf{B}\mathbb{Z}^n = \left\{ \sum_{i=1}^n x_i \cdot \mathbf{b}_i : x_i \in \mathbb{Z} \right\}$$

- It can be generated by  $\mathbf{B}\mathbb{Z}^n$  if  $\mathbf{B}$  is a matrix of independent vectors.
- It is not a vector space and it can have many basis. We do not change the basis by multiplying it by a unimodular matrix  $\mathbf{U}$  s.t.  $|\det(\mathbf{U})| = 1$ .



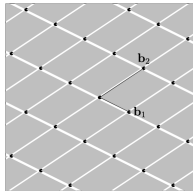
## Invariants of the lattice

The volume of the fundamental parallelepiped  $\mathbf{B} \left[ -\frac{1}{2}, \frac{1}{2} \right)^n$  of a lattice is the same for all basis



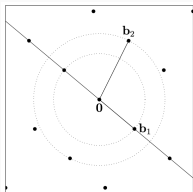
# Invariants of the lattice

The volume of the fundamental parallelepiped  $B\left[-\frac{1}{2}, \frac{1}{2}\right)^n$  of a lattice is the same for all basis



Minima of the lattice: there is a short non-zero lattice point

$$\|\mathbf{v}\| \leq \sqrt{n} \det(L)^{1/n}$$



# Hard Lattice Problems

## Short Vector Problem (SVP)

- Given a lattice  $L$  defined by its basis  $\mathbf{B}$ , find a non-zero lattice points ? or an approximation of it ?
- Approximating the problem up to a constant factor is NP-hard..
- Cryptographic instances requires polynomial factor approximation

# Hard Lattice Problems

## Short Vector Problem (SVP)

- Given a lattice  $L$  defined by its basis  $\mathbf{B}$ , find a non-zero lattice points ? or an approximation of it ?
- Approximating the problem up to a constant factor is NP-hard..
- Cryptographic instances requires polynomial factor approximation

## Closest Vector Problem (CVP)

- Given a lattice  $L$  defined by its basis  $\mathbf{B}$  and a point  $\mathbf{t}$  in the ambient space of  $L$ , find a lattice point close to  $\mathbf{t}$  ? or not too far from it ?
- This problem is hard that SVP...

# Hard Lattice Problems

## Short Vector Problem (SVP)

- Given a lattice  $L$  defined by its basis  $\mathbf{B}$ , find a non-zero lattice points ? or an approximation of it ?
- Approximating the problem up to a constant factor is NP-hard..
- Cryptographic instances requires polynomial factor approximation

## Closest Vector Problem (CVP)

- Given a lattice  $L$  defined by its basis  $\mathbf{B}$  and a point  $\mathbf{t}$  in the ambient space of  $L$ , find a lattice point close to  $\mathbf{t}$  ? or not too far from it ?
- This problem is hard that SVP...

## Short Independent Vectors Problem (SIVP)

Given a lattice  $L$  defined by its basis  $\mathbf{B}$ , find a set of  $n$  independent vectors in  $L$  ? Or an approximation of the shortest basis ? (Warning, we do not ask to find a basis... )

# LLL Algorithm

## **Motivation for cryptanalysis**

This algorithm has been used in cryptanalysis: each time you have a find a short linear integer relation for some values, LLL or variants are helpful

# LLL Algorithm

## Motivation for cryptanalysis

This algorithm has been used in cryptanalysis: each time you have to find a short linear integer relation for some values, LLL or variants are helpful

## Algorithm

- The LLL (Lenstra, Lenstra, Lovàsz) algorithm returns in polynomial-time a basis with basis vectors as orthogonal as possible and short (by an exponential factor  $2^{(n-1)/2}$  ...)

# LLL Algorithm

## Motivation for cryptanalysis

This algorithm has been used in cryptanalysis: each time you have to find a short linear integer relation for some values, LLL or variants are helpful

## Algorithm

- The LLL (Lenstra, Lenstra, Lovàsz) algorithm returns in polynomial-time a basis with basis vectors as orthogonal as possible and short (by an exponential factor  $2^{(n-1)/2}$  ...)
- Idea: use the Gram-Schmidt orthogonalization process and round fractions by integers

# LLL Algorithm

## Motivation for cryptanalysis

This algorithm has been used in cryptanalysis: each time you have to find a short linear integer relation for some values, LLL or variants are helpful

## Algorithm

- The LLL (Lenstra, Lenstra, Lovàsz) algorithm returns in polynomial-time a basis with basis vectors as orthogonal as possible and short (by an exponential factor  $2^{(n-1)/2}$  ...)
- Idea: use the Gram-Schmidt orthogonalization process and round fractions by integers
- Since the new basis has the same determinant as the starting basis, the volume is constant, it is important that the Gram-Schmidt vectors do not decrease too much

## Motivation for cryptanalysis

This algorithm has been used in cryptanalysis: each time you have to find a short linear integer relation for some values, LLL or variants are helpful

## Algorithm

- The LLL (Lenstra, Lenstra, Lovàsz) algorithm returns in polynomial-time a basis with basis vectors as orthogonal as possible and short (by an exponential factor  $2^{(n-1)/2}$  ...)
- Idea: use the Gram-Schmidt orthogonalization process and round fractions by integers
- Since the new basis has the same determinant as the starting basis, the volume is constant, it is important that the Gram-Schmidt vectors do not decrease too much
- More efficient algorithms by Schnorr achieve better tradeoff: smaller approximation factors but in exponential time ...

Ajtai result: SIS problem

## Ajtai result: SIS problem

- Short Integer Solution (SIS) problem: given a matrix  $\mathbf{A} \in \mathbb{Z}^{n \times m}$ , where  $m > n$ , and a prime  $q$ , find a short non-zero vector  $\mathbf{z}$  s.t.  $\|\mathbf{z}\| < \beta$  and  $\mathbf{Az} = \mathbf{0} \pmod{q}$ .

## Ajtai result: SIS problem

- Short Integer Solution (SIS) problem: given a matrix  $\mathbf{A} \in \mathbb{Z}^{n \times m}$ , where  $m > n$ , and a prime  $q$ , find a short non-zero vector  $\mathbf{z}$  s.t.  $\|\mathbf{z}\| < \beta$  and  $\mathbf{Az} = \mathbf{0} \pmod{q}$ .
- The kernel of  $\mathbf{A}$  is very large  $q^{m-n}$  and find a short vector in it

## Ajtai result: SIS problem

- Short Integer Solution (SIS) problem: given a matrix  $\mathbf{A} \in \mathbb{Z}^{n \times m}$ , where  $m > n$ , and a prime  $q$ , find a short non-zero vector  $\mathbf{z}$  s.t.  $\|\mathbf{z}\| < \beta$  and  $\mathbf{Az} = \mathbf{0} \pmod{q}$ .
- The kernel of  $\mathbf{A}$  is very large  $q^{m-n}$  and find a short vector in it
- Ajtai shows that this average-case problem (define a probability distribution on the random instances), is as hard as SIVP.

# Ajtai and Regev breakthroughs

## Ajtai result: SIS problem

- Short Integer Solution (SIS) problem: given a matrix  $\mathbf{A} \in \mathbb{Z}^{n \times m}$ , where  $m > n$ , and a prime  $q$ , find a short non-zero vector  $\mathbf{z}$  s.t.  $\|\mathbf{z}\| < \beta$  and  $\mathbf{Az} = \mathbf{0} \pmod{q}$ .
- The kernel of  $\mathbf{A}$  is very large  $q^{m-n}$  and find a short vector in it
- Ajtai shows that this average-case problem (define a probability distribution on the random instances), is as hard as SIVP.
- SIS can be used to construct signature scheme, but it cannot be used to construct public-key encryption

## Regev result: LWE problem

## Ajtai result: SIS problem

- Short Integer Solution (SIS) problem: given a matrix  $\mathbf{A} \in \mathbb{Z}^{n \times m}$ , where  $m > n$ , and a prime  $q$ , find a short non-zero vector  $\mathbf{z}$  s.t.  $\|\mathbf{z}\| < \beta$  and  $\mathbf{Az} = \mathbf{0} \pmod{q}$ .
- The kernel of  $\mathbf{A}$  is very large  $q^{m-n}$  and find a short vector in it
- Ajtai shows that this average-case problem (define a probability distribution on the random instances), is as hard as SIVP.
- SIS can be used to construct signature scheme, but it cannot be used to construct public-key encryption

## Regev result: LWE problem

- Learning with Errors (LWE) problem: given a matrix  $\mathbf{A} \in \mathbb{Z}^{m \times n}$ , where  $m > n$ , a prime  $q$ , and a vector  $\mathbf{t} \in (\mathbb{Z}/q\mathbb{Z})^m$ ,  $\mathbf{t} = \mathbf{As} + \mathbf{e}$  where  $s \in (\mathbb{Z}/q\mathbb{Z})^n$  and  $\mathbf{e} \in [\beta, \beta]^m$ , recover  $\mathbf{s}$ .

## Ajtai result: SIS problem

- Short Integer Solution (SIS) problem: given a matrix  $\mathbf{A} \in \mathbb{Z}^{n \times m}$ , where  $m > n$ , and a prime  $q$ , find a short non-zero vector  $\mathbf{z}$  s.t.  $\|\mathbf{z}\| < \beta$  and  $\mathbf{Az} = \mathbf{0} \pmod{q}$ .
- The kernel of  $\mathbf{A}$  is very large  $q^{m-n}$  and find a short vector in it
- Ajtai shows that this average-case problem (define a probability distribution on the random instances), is as hard as SIVP.
- SIS can be used to construct signature scheme, but it cannot be used to construct public-key encryption

## Regev result: LWE problem

- Learning with Errors (LWE) problem: given a matrix  $\mathbf{A} \in \mathbb{Z}^{m \times n}$ , where  $m > n$ , a prime  $q$ , and a vector  $\mathbf{t} \in (\mathbb{Z}/q\mathbb{Z})^m$ ,  $\mathbf{t} = \mathbf{As} + \mathbf{e}$  where  $s \in (\mathbb{Z}/q\mathbb{Z})^n$  and  $e \in [\beta, \beta]^m$ , recover  $\mathbf{s}$ .
- Given noisy linear equations, solve the linear system ...

# Ajtai and Regev breakthroughs

## Ajtai result: SIS problem

- Short Integer Solution (SIS) problem: given a matrix  $\mathbf{A} \in \mathbb{Z}^{n \times m}$ , where  $m > n$ , and a prime  $q$ , find a short non-zero vector  $\mathbf{z}$  s.t.  $\|\mathbf{z}\| < \beta$  and  $\mathbf{Az} = \mathbf{0} \pmod{q}$ .
- The kernel of  $\mathbf{A}$  is very large  $q^{m-n}$  and find a short vector in it
- Ajtai shows that this average-case problem (define a probability distribution on the random instances), is as hard as SIVP.
- SIS can be used to construct signature scheme, but it cannot be used to construct public-key encryption

## Regev result: LWE problem

- Learning with Errors (LWE) problem: given a matrix  $\mathbf{A} \in \mathbb{Z}^{m \times n}$ , where  $m > n$ , a prime  $q$ , and a vector  $\mathbf{t} \in (\mathbb{Z}/q\mathbb{Z})^m$ ,  $\mathbf{t} = \mathbf{As} + \mathbf{e}$  where  $s \in (\mathbb{Z}/q\mathbb{Z})^n$  and  $e \in [\beta, \beta]^m$ , recover  $\mathbf{s}$ .
- Given noisy linear equations, solve the linear system ...
- Regev shows that this problem is as hard as GapCVP quantumly

- Shor is a very interesting algorithm and it still works even if there is many errors

# Conclusion

- Shor is a very interesting algorithm and it still works even if there is many errors
- Shor algorithm for ECC are still very low: ECC have shorter keys 256 bits, but we need to compute modular inverse

- Shor is a very interesting algorithm and it still works even if there is many errors
- Shor algorithm for ECC are still very low: ECC have shorter keys 256 bits, but we need to compute modular inverse
- It is important to look at the security of post-quantum cryptosystem using quantum algorithms since they have to resist such adversaries

# Conclusion

- Shor is a very interesting algorithm and it still works even if there is many errors
- Shor algorithm for ECC are still very low: ECC have shorter keys 256 bits, but we need to compute modular inverse
- It is important to look at the security of post-quantum cryptosystem using quantum algorithms since they have to resist such adversaries
- Finally, it is important to look at the security of cryptosystems since sometimes more information are available and not only the hard mathematical problems on which they are based