CS621/CSL611
Quantum Computing For Computer Scientists

Quantum Search

Dhiman Saha

Winter 2024

IIT Bhilai

Revisiting Simon's Algorithm

From The Index View Perspective

Problem Definition

Assumptions:

- Given any $u \in \{0,1\}^n$,
  can efficiently compute $f(u)$.
- Nonzero $s \in \{0,1\}^n$.
- $f(u) = f(u \oplus s)$ for all u.
- f has no other collisions.

Goal: Figure out s.

Problem Definition

Assumptions:

- Given any $u \in \{0,1\}^n$,
  can efficiently compute $f(u)$.
- Nonzero $s \in \{0,1\}^n$.
- $f(u) = f(u \oplus s)$ for all u.
- f has no other collisions.

Goal: Figure out s.

Non-quantum algorithm to find s:
compute f for many inputs,
hope to find collision.

Problem Definition

Assumptions:

- Given any $u \in \{0,1\}^n$,
  can efficiently compute $f(u)$.
- Nonzero $s \in \{0,1\}^n$.
- $f(u) = f(u \oplus s)$ for all u.
- f has no other collisions.

Goal: Figure out s.

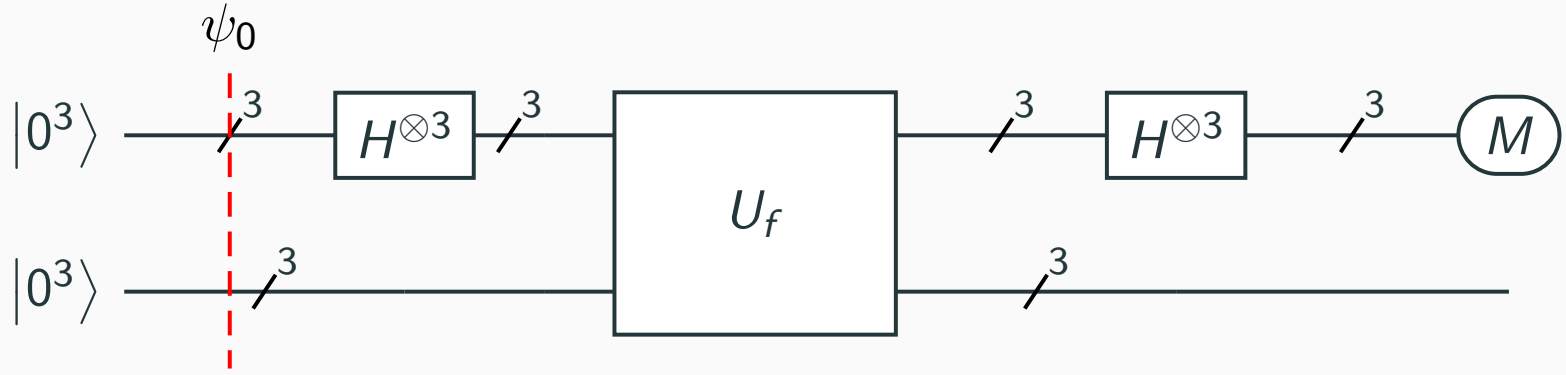
Non-quantum algorithm to find s:
compute f for many inputs,
hope to find collision.

Simon's algorithm finds s with
$\approx n$ quantum evaluations of f.

Step 1. Set up pure zero state

1, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0.

- This example is for a function f with 3-bit input and 3-bit output
- Each column is a parallel universe.
- Step 3 will apply the function f (a specific function in this example), computing $f(u)$ in universe u.

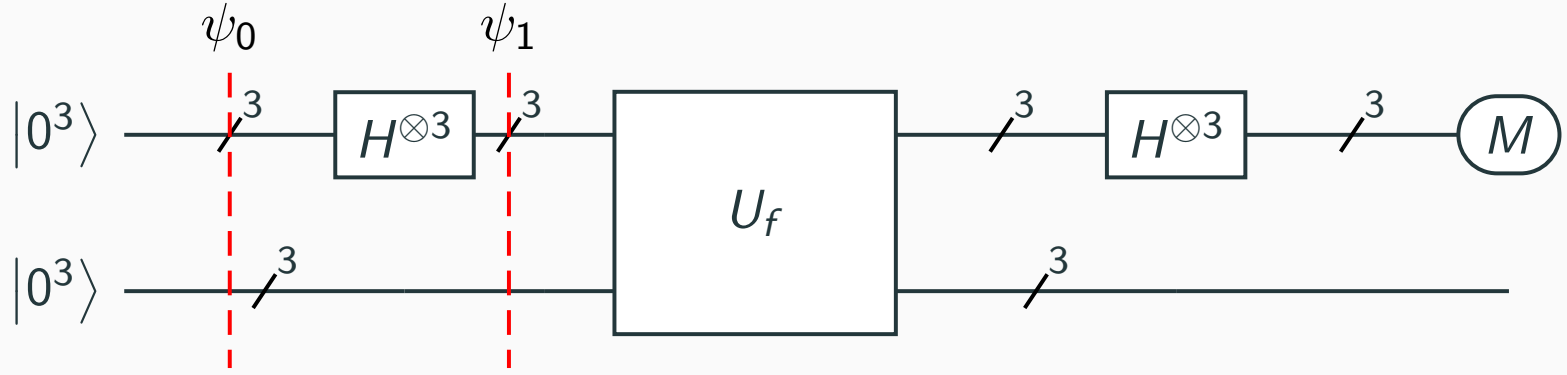


Adapted from Bernstein's Invited Talk at Indocrypt 2021

Step 2.0. Hadamard$_0$

1, 1, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0.

- This example is for a function f with 3-bit input and 3-bit output
- Each column is a parallel universe.
- Step 3 will apply the function f (a specific function in this example), computing $f(u)$ in universe u.

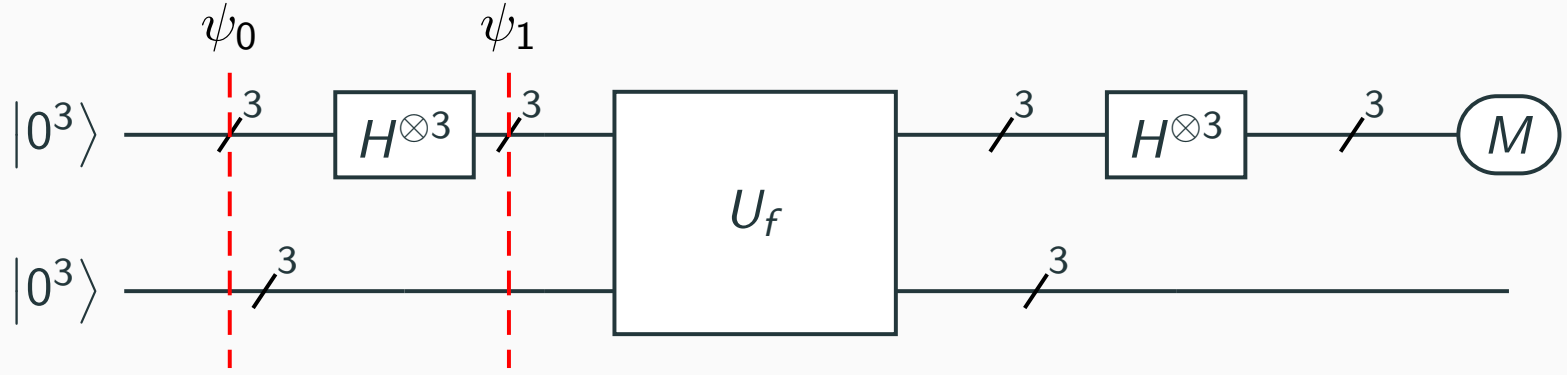


Adapted from Bernstein's Invited Talk at Indocrypt 2021

Step 2.1. Hadamard$_1$

1, 1, 1, 1, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0.

- This example is for a function f with 3-bit input and 3-bit output
- Each column is a parallel universe.
- Step 3 will apply the function f (a specific function in this example), computing $f(u)$ in universe u.

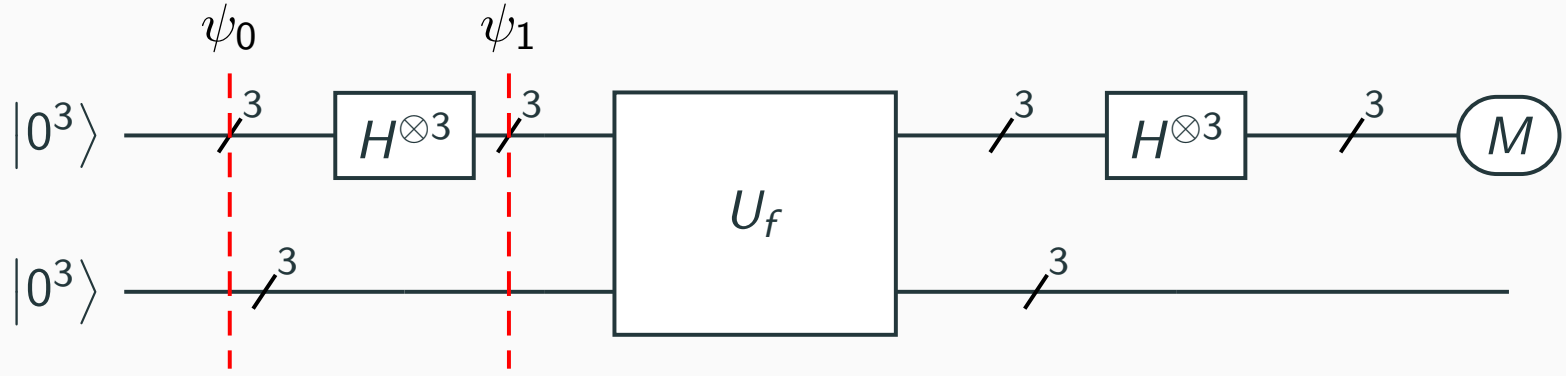


Adapted from Bernstein's Invited Talk at Indocrypt 2021

Step 2.2. Hadamard$_2$

1, 1, 1, 1, 1, 1, 1, 1,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0.

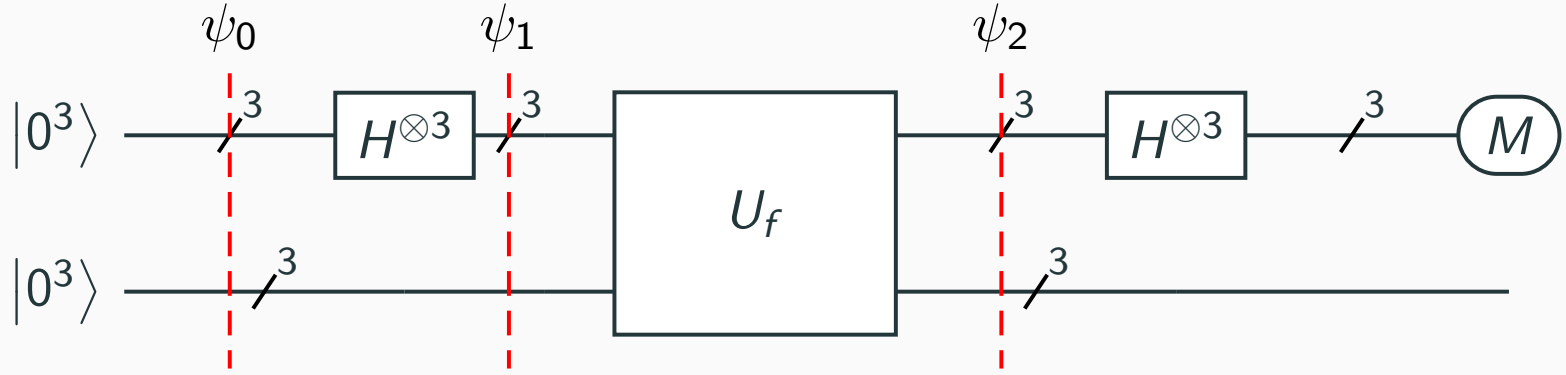
- This example is for a function f with 3-bit input and 3-bit output
- Each column is a parallel universe.
- Step 3 will apply the function f (a specific function in this example), computing $f(u)$ in universe u.



Adapted from Bernstein's Invited Talk at Indocrypt 2021

1, 0, 1, 0, 1, 0, 1, 0,
0, 1, 0, 1, 0, 1, 0, 1,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0.

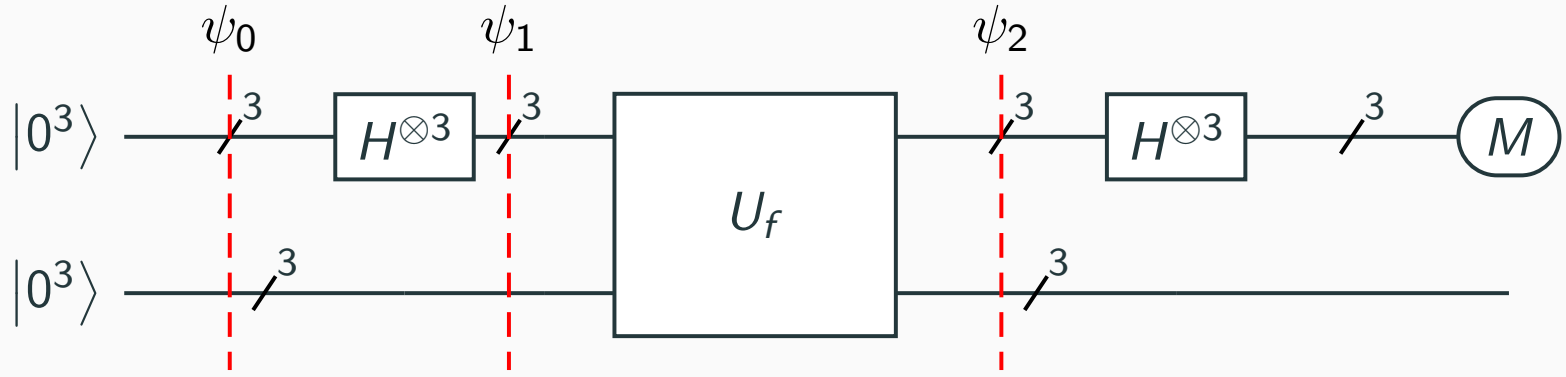
- Each column is a parallel universe performing its own computations



Adapted from Bernstein's Invited Talk at Indocrypt 2021

1, 0, 0, 0, 1, 0, 0, 0,
0, 1, 0, 0, 0, 1, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 1, 0, 0, 0, 1, 0,
0, 0, 0, 1, 0, 0, 0, 1,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0.

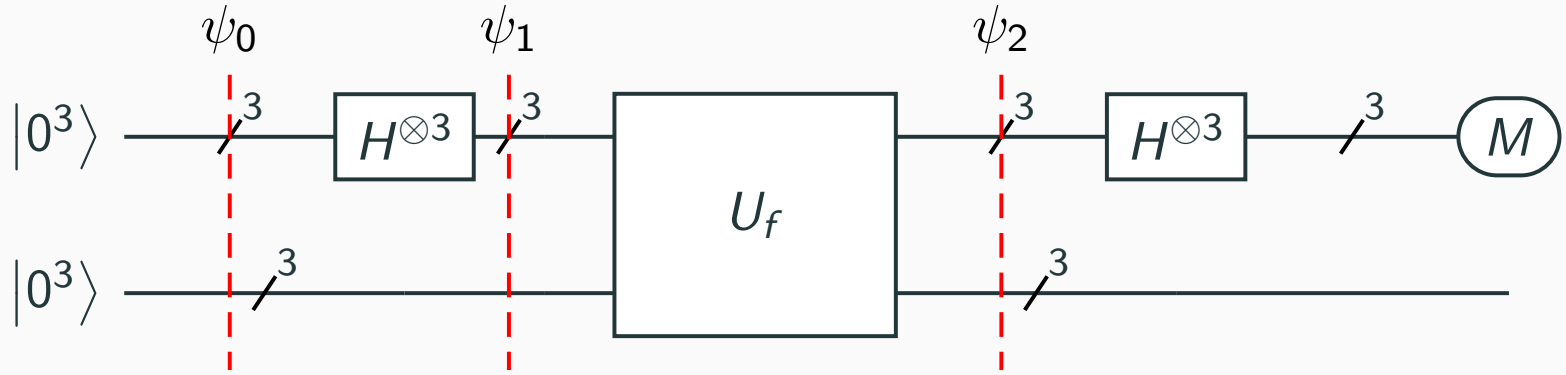
- Each column is a parallel universe performing its own computations



Adapted from Bernstein's Invited Talk at Indocrypt 2021

1, 0, 0, 0, 0, 0, 0, 0,
0, 1, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 1, 0, 0, 0,
0, 0, 0, 0, 0, 1, 0, 0,
0, 0, 1, 0, 0, 0, 0, 0,
0, 0, 0, 1, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 1, 0,
0, 0, 0, 0, 0, 0, 0, 1.

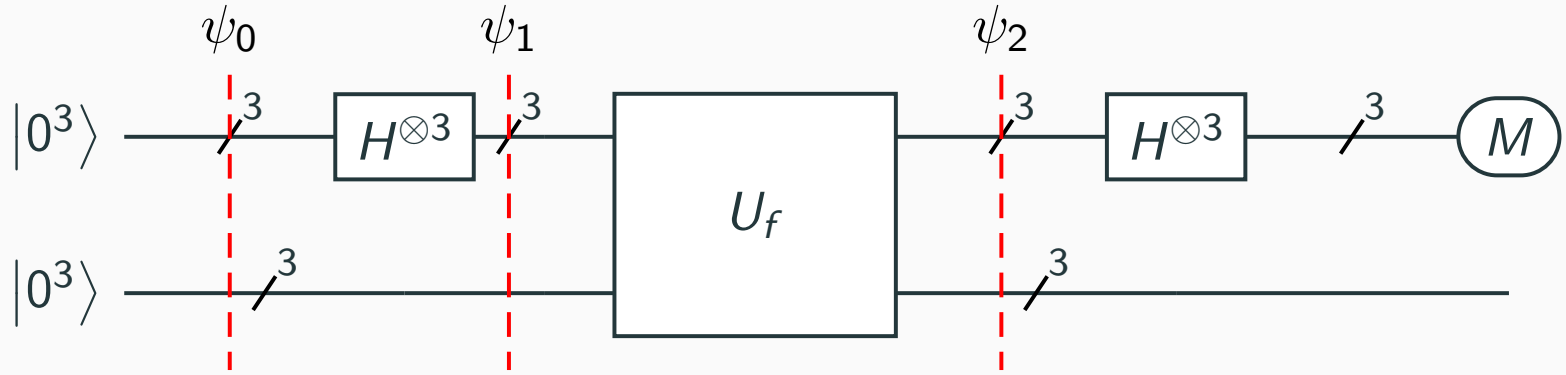
- Each column is a parallel universe performing its own computations



Adapted from Bernstein's Invited Talk at Indocrypt 2021

1, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 1, 0, 0,
0, 0, 0, 0, 1, 0, 0, 0,
0, 1, 0, 0, 0, 0, 0, 0,
0, 0, 1, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 1,
0, 0, 0, 0, 0, 0, 1, 0,
0, 0, 0, 1, 0, 0, 0, 0.

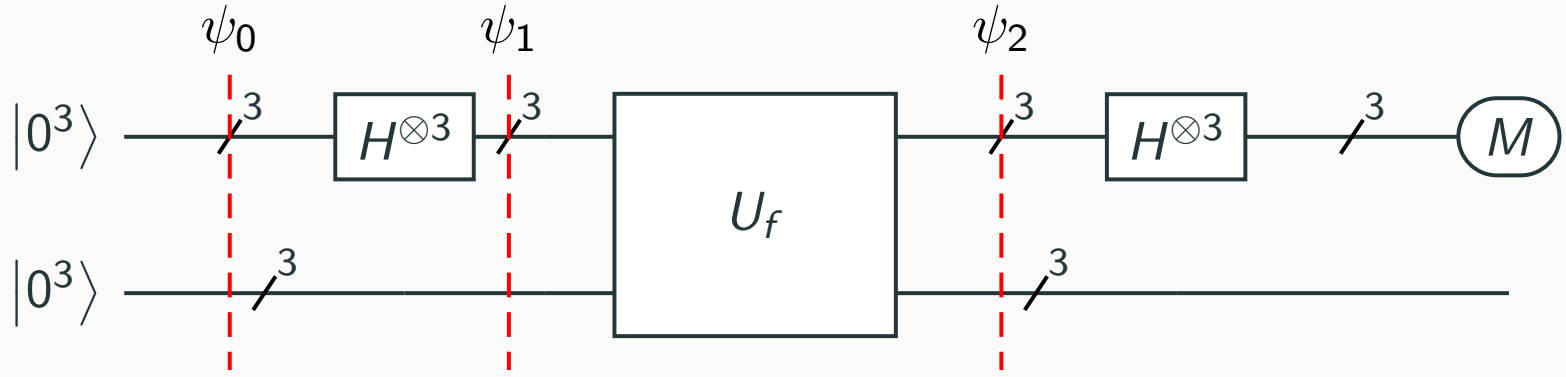
- Each column is a parallel universe performing its own computations



Adapted from Bernstein's Invited Talk at Indocrypt 2021

1, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 1, 0, 0,
0, 0, 0, 0, 1, 0, 0, 0,
0, 1, 0, 0, 0, 0, 0, 0,
0, 0, 1, 0, 0, 0, 0, 1,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 1, 0, 0, 1, 0,
0, 0, 0, 0, 0, 0, 0, 0.

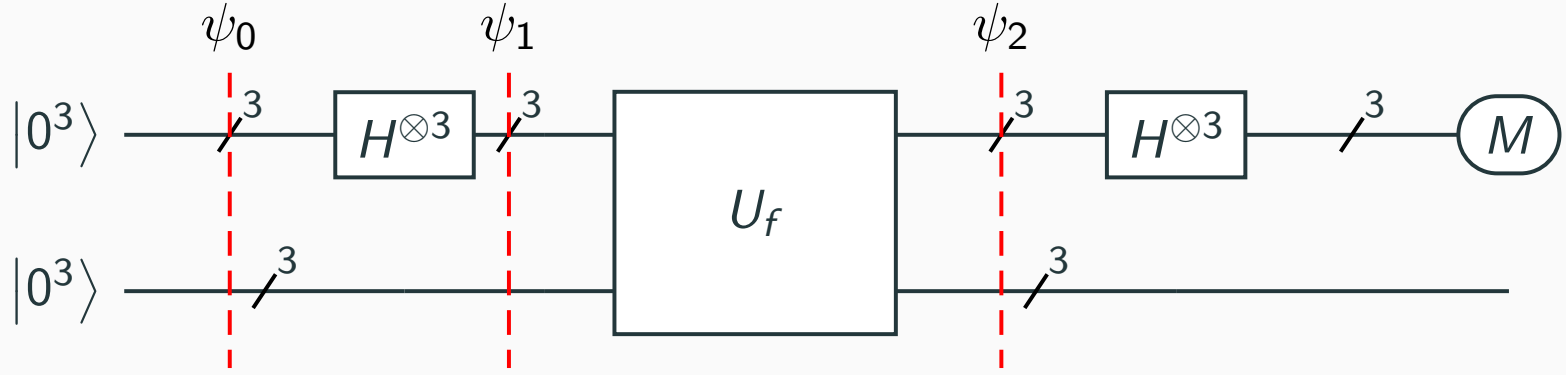
- Each column is a parallel universe performing its own computations



Adapted from Bernstein's Invited Talk at Indocrypt 2021

0, 0, 0, 0, 0, 1, 0, 0,
1, 0, 0, 0, 0, 0, 0, 0,
0, 1, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 1, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 1, 0, 0, 0, 0, 1,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 1, 0, 0, 1, 0.

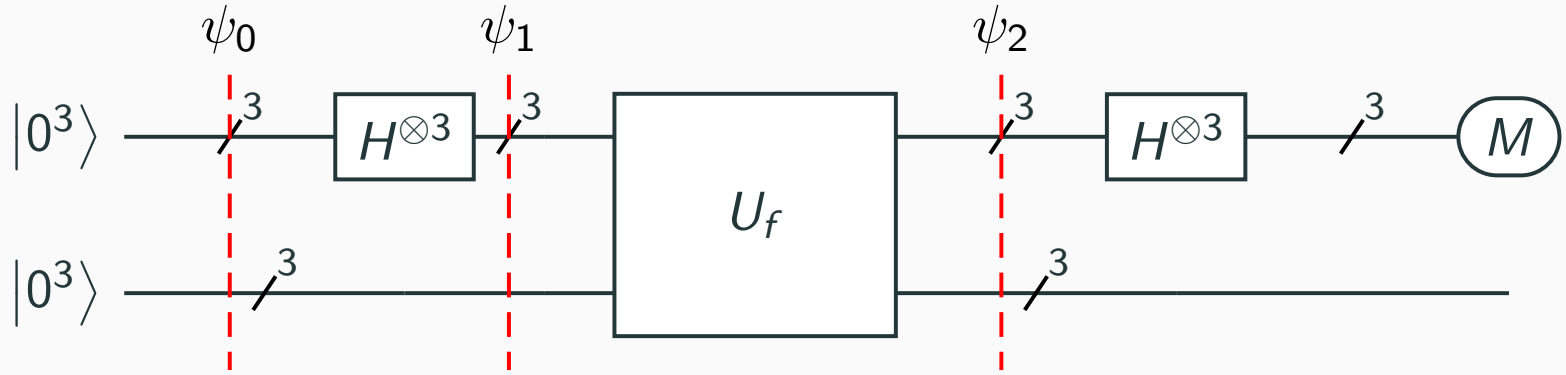
- Each column is a parallel universe performing its own computations



Adapted from Bernstein's Invited Talk at Indocrypt 2021

0, 1, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 1, 0, 0, 0,
0, 0, 0, 0, 0, 1, 0, 0,
1, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 1, 0, 0, 1, 0,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 1, 0, 0, 0, 0, 1.

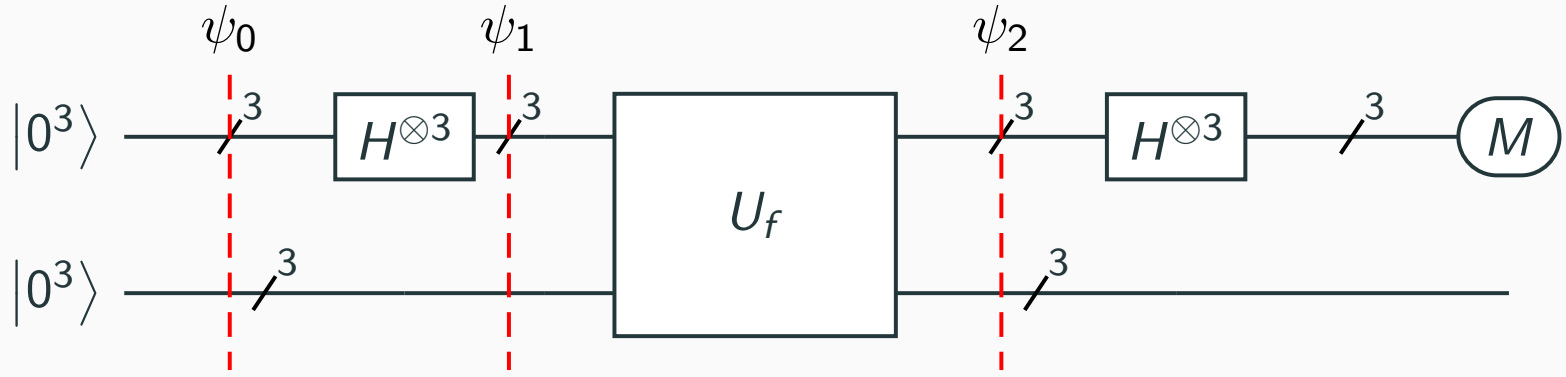
- Each column is a parallel universe performing its own computations



Adapted from Bernstein's Invited Talk at Indocrypt 2021

0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 1, 0, 0, 1, 0,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 1, 0, 0, 0, 0, 1,
0, 1, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 1, 0, 0, 0,
0, 0, 0, 0, 0, 1, 0, 0,
1, 0, 0, 0, 0, 0, 0, 0.

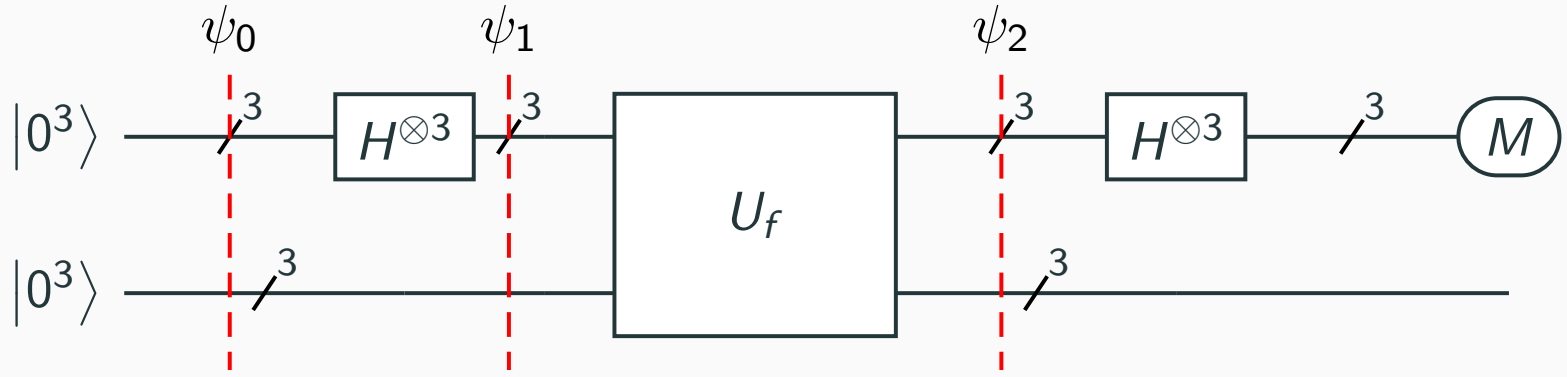
- Each column is a parallel universe performing its own computations



Adapted from Bernstein's Invited Talk at Indocrypt 2021

0, 0, 0, 0, 0, 0, 1, 0,
0, 0, 0, 1, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 1,
0, 0, 1, 0, 0, 0, 0, 0,
0, 1, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 1, 0, 0, 0,
0, 0, 0, 0, 0, 1, 0, 0,
1, 0, 0, 0, 0, 0, 0, 0.

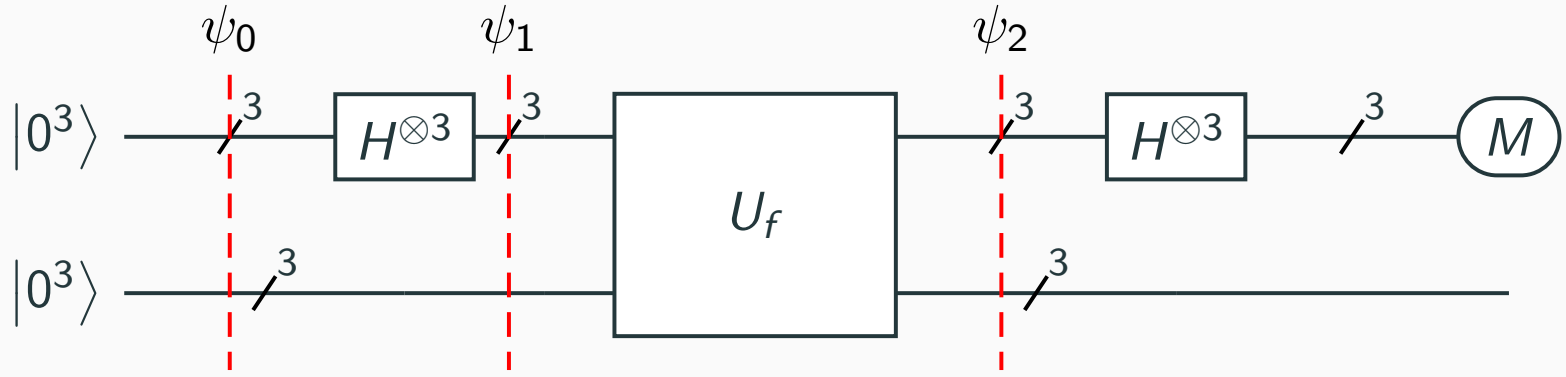
- Each column is a parallel universe performing its own computations



Adapted from Bernstein's Invited Talk at Indocrypt 2021

0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 1, 0, 0, 1, 0,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 1, 0, 0, 0, 0, 1,
0, 1, 0, 0, 1, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,
1, 0, 0, 0, 0, 1, 0, 0.

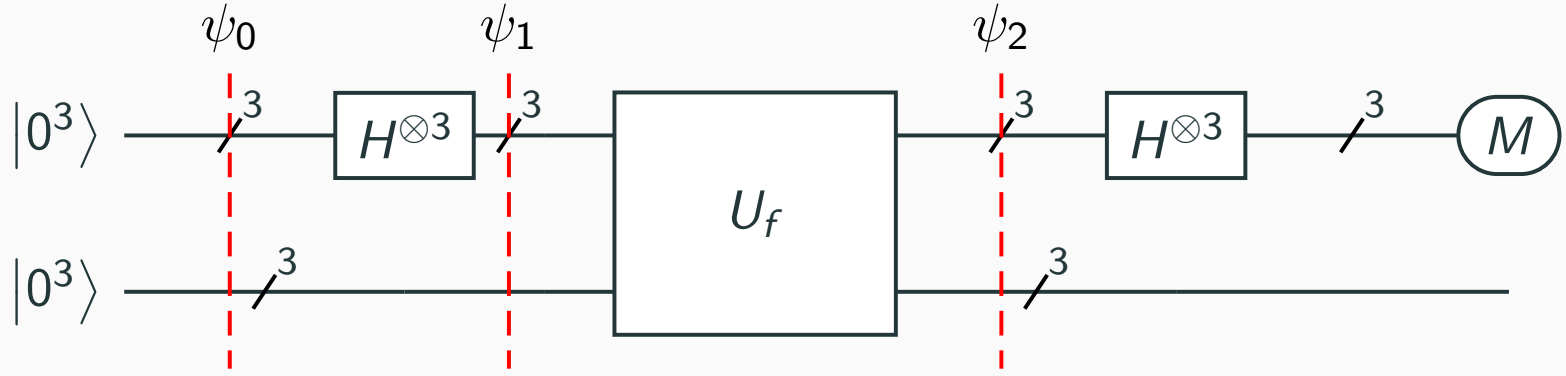
- Each column is a parallel universe performing its own computations



Adapted from Bernstein's Invited Talk at Indocrypt 2021

0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 1, 0, 0, 1, 0,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 1, 0, 0, 0, 0, 1,
0, 1, 0, 0, 1, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,
1, 0, 0, 0, 0, 1, 0, 0.

- Each column is a parallel universe performing its own computations
- Note: u and $u \oplus 101$ match

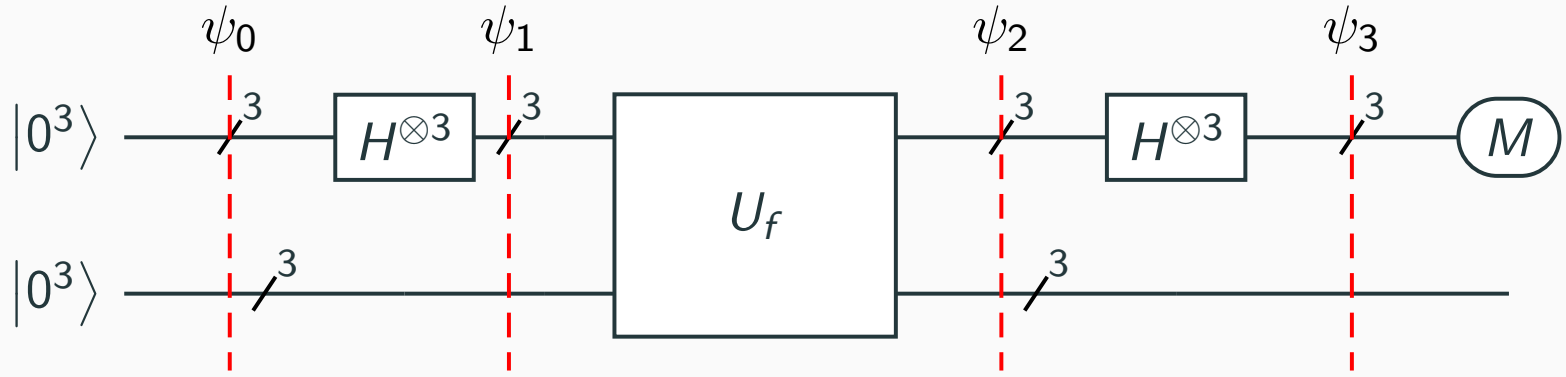


Adapted from Bernstein's Invited Talk at Indocrypt 2021

Step 4.0. Hadamard$_0$

0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 1, 0, 0, 1, 0,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 1, 0, 0, 0, 0, 1,
0, 1, 0, 0, 1, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0,
1, 0, 0, 0, 0, 1, 0, 0.

- Notation: $\overline{1}$ means -1

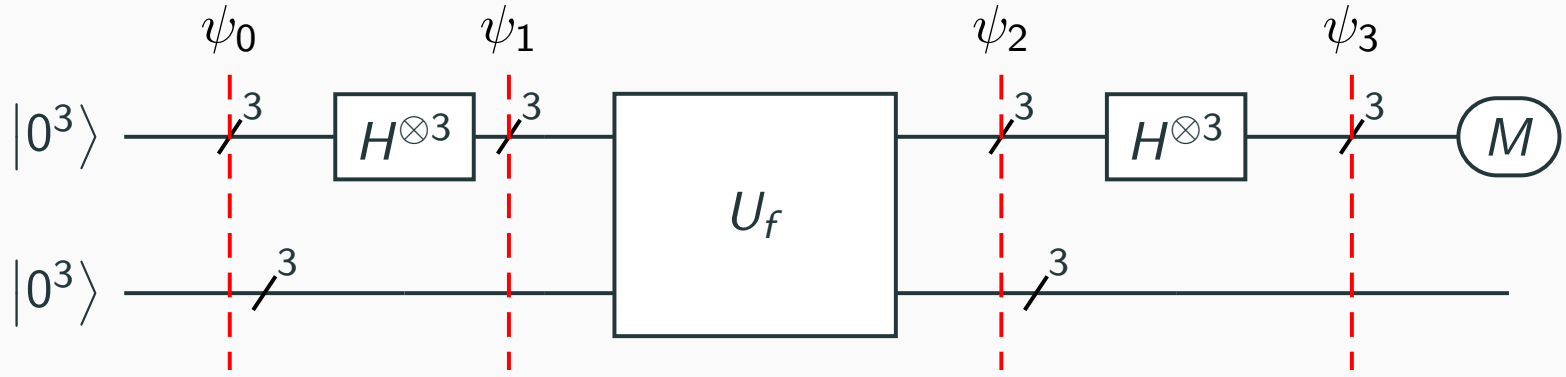


Adapted from Bernstein's Invited Talk at Indocrypt 2021

Step 4.1. Hadamard$_1$

$$
\begin{array}{cccccccc}
0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, \\
0, & 0, & 1, & \overline{1}, & 0, & 0, & 1, & 1, \\
0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, \\
0, & 0, & 1, & 1, & 0, & 0, & 1, & \overline{1}, \\
1, & \overline{1}, & 0, & 0, & 1, & 1, & 0, & 0, \\
0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, \\
0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, \\
1, & 1, & 0, & 0, & 1, & \overline{1}, & 0, & 0.
\end{array}
$$

- Notation: $\overline{1}$ means -1

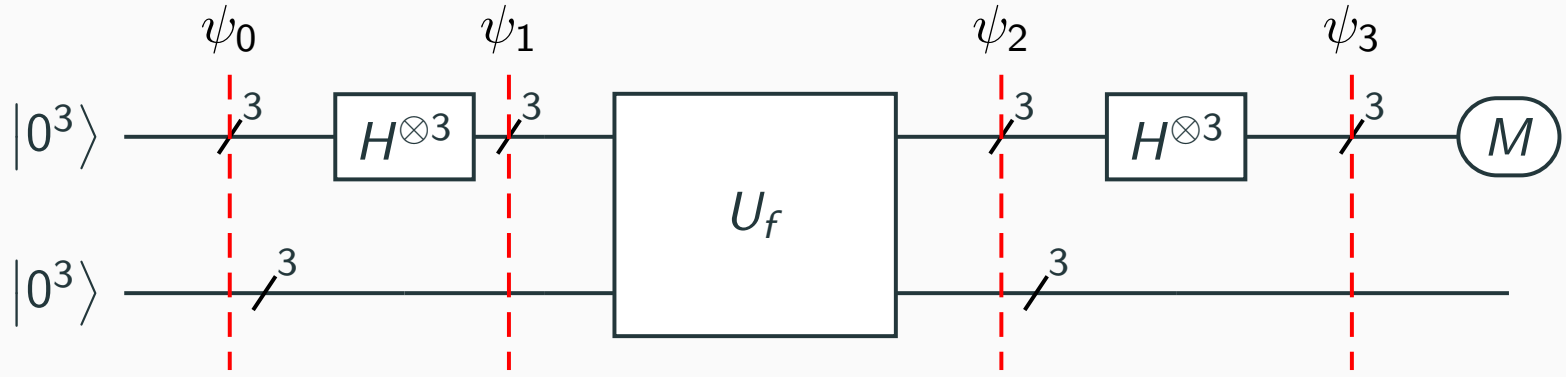


Adapted from Bernstein's Invited Talk at Indocrypt 2021

Step 4.2. Hadamard$_2$

$$
\begin{array}{cccccccc}
0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, \\
1, & \overline{1}, & \overline{1}, & 1, & 1, & 1, & \overline{1}, & \overline{1}, \\
0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, \\
1, & 1, & \overline{1}, & \overline{1}, & 1, & \overline{1}, & \overline{1}, & 1, \\
1, & \overline{1}, & 1, & \overline{1}, & 1, & 1, & 1, & 1, \\
0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, \\
0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, \\
1, & 1, & 1, & 1, & 1, & \overline{1}, & 1, & \overline{1}.
\end{array}
$$

- Notation: $\overline{1}$ means -1

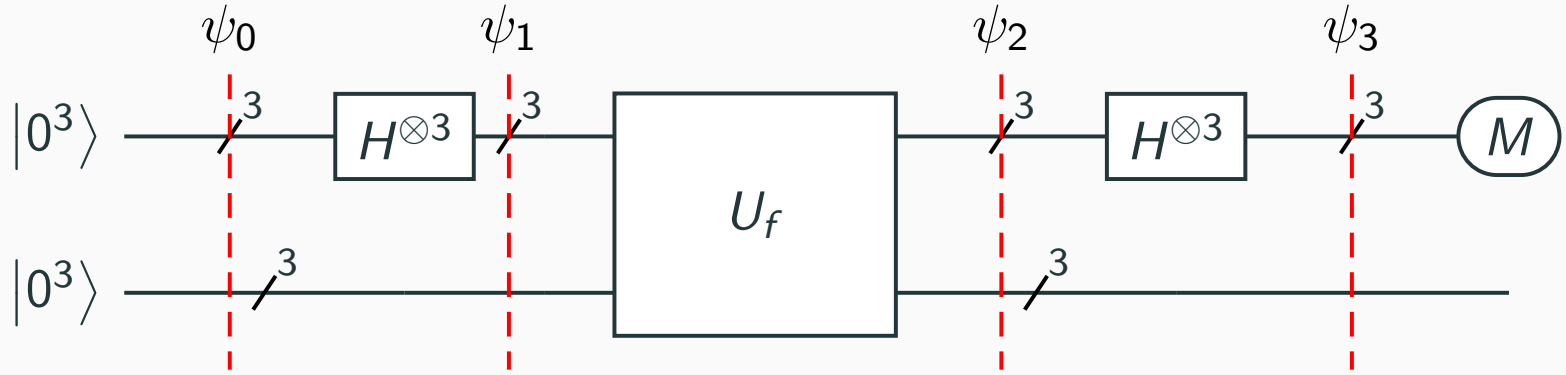


Adapted from Bernstein's Invited Talk at Indocrypt 2021

Step 5. Measure

$0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,$
$2,\ 0,\ \overline{2},\ 0,\ 0,\ \overline{2},\ 0,\ 2,$
$0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,$
$2,\ 0,\ \overline{2},\ 0,\ 0,\ 2,\ 0,\ \overline{2},$
$2,\ 0,\ 2,\ 0,\ 0,\ \overline{2},\ 0,\ \overline{2},$
$0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,$
$0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,$
$2,\ 0,\ 2,\ 0,\ 0,\ 2,\ 0,\ 2.$

- Notation: $\overline{1}$ means -1
- Obtain some information about the *period* of f: a random vector **orthogonal** to 101

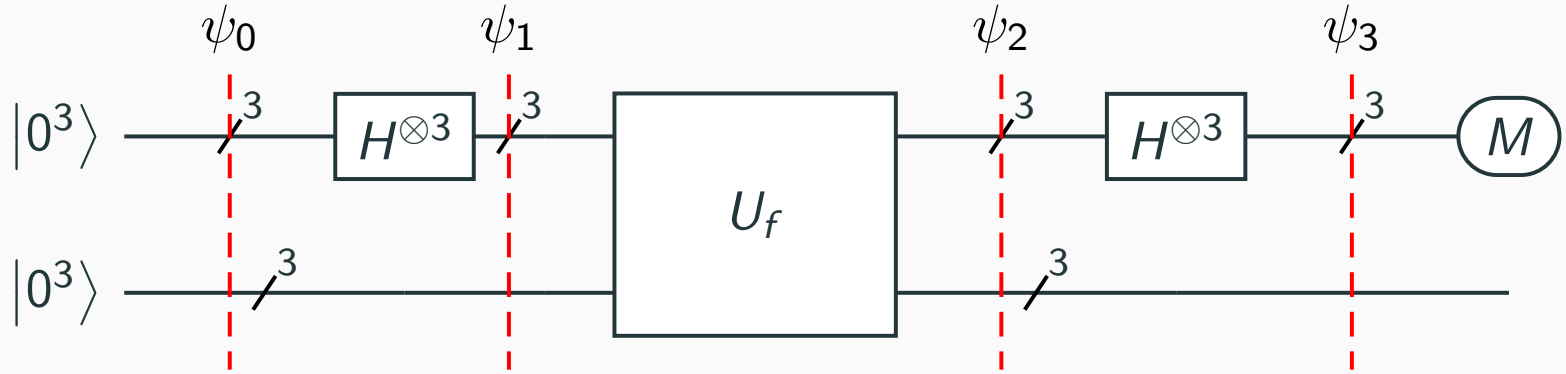


Adapted from Bernstein's Invited Talk at Indocrypt 2021

Step 5. Measure

$0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,$
$2,\ 0,\ \overline{2},\ 0,\ 0,\ \overline{2},\ 0,\ 2,$
$0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,$
$2,\ 0,\ \overline{2},\ 0,\ 0,\ 2,\ 0,\ \overline{2},$
$2,\ 0,\ 2,\ 0,\ 0,\ \overline{2},\ 0,\ \overline{2},$
$0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,$
$0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,\ 0,$
$2,\ 0,\ 2,\ 0,\ 0,\ 2,\ 0,\ 2.$

- Notation: $\overline{1}$ means -1
- Obtain some information about the *period* of f: a random vector **orthogonal** to 101
- Repeat to figure out 101



Adapted from Bernstein's Invited Talk at Indocrypt 2021