





$t_k, k$





$t_k, k$

$$(\alpha_i \stackrel{s}{\leftarrow} \{0, \frac{\pi}{4} \dots \frac{7\pi}{4}\})_{i=1}^{n-1}$$





$t_k, k$



$$(\alpha_i \stackrel{s}{\leftarrow} \{0, \frac{\pi}{4} \dots \frac{7\pi}{4}\})_{i=1}^{n-1}$$

$k, (\alpha_i)$



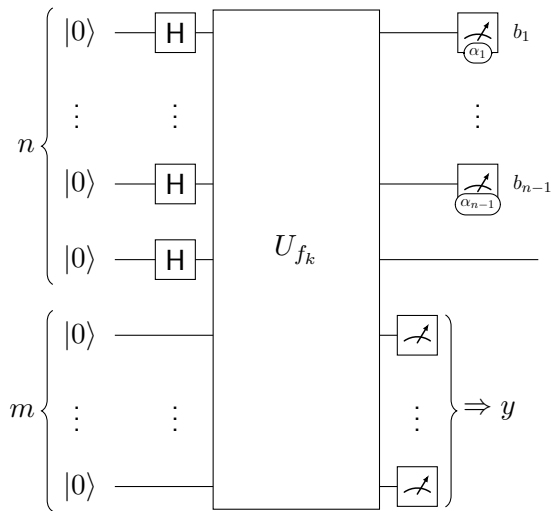


$t_k, k$



$k, (\alpha_i)$

Compute circuit



$$|0\rangle^{\otimes n} |0\rangle^{\otimes m}$$

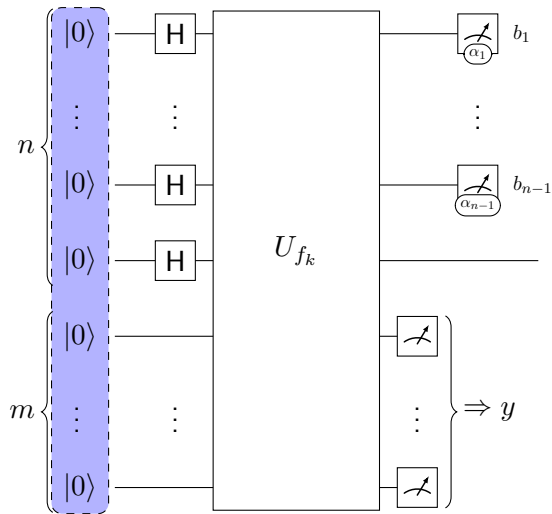


$t_k, k$



$k, (\alpha_i)$

Compute circuit



$$|0\rangle^{\otimes n} |0\rangle^{\otimes m} \Rightarrow \sum_x |x\rangle |0\rangle^{\otimes m}$$

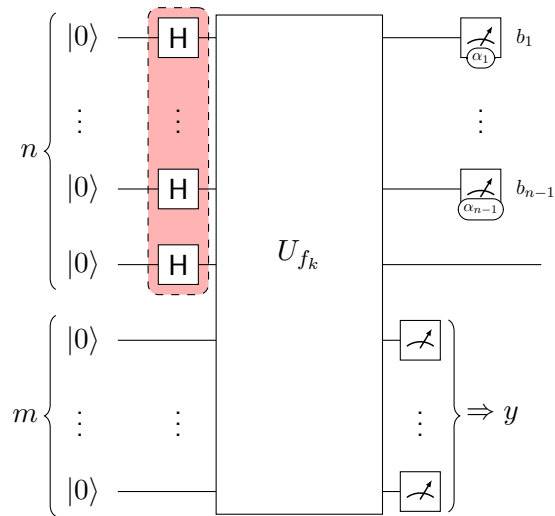


$t_k, k$



$k, (\alpha_i)$

Compute circuit



$$|0\rangle^{\otimes n} |0\rangle^{\otimes m} \Rightarrow \sum_x |x\rangle |0\rangle^{\otimes m} \Rightarrow \sum_x |x\rangle |f_k(x)\rangle$$



$t_k, k$

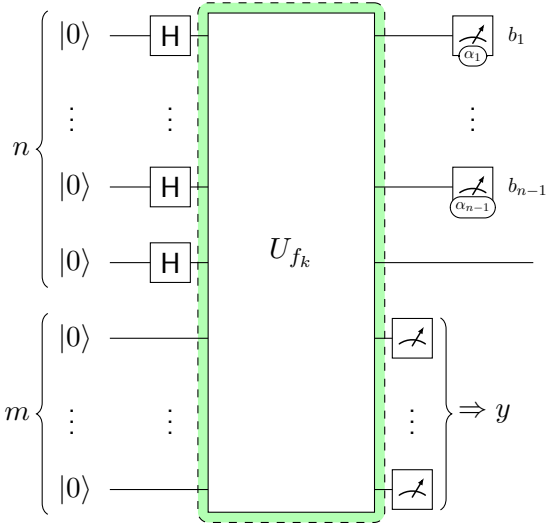


$$(\alpha_i \stackrel{s}{\leftarrow} \{0, \frac{\pi}{4} \dots \frac{7\pi}{4}\}_{i=1}^{n-1})$$

$k, (\alpha_i)$



Compute circuit





$$|0\rangle^{\otimes n} |0\rangle^{\otimes m} \Rightarrow \sum_x |x\rangle |0\rangle^{\otimes m} \Rightarrow \sum_x |x\rangle |f_k(x)\rangle = \sum_y (|x\rangle + |x'\rangle) \otimes |y\rangle$$

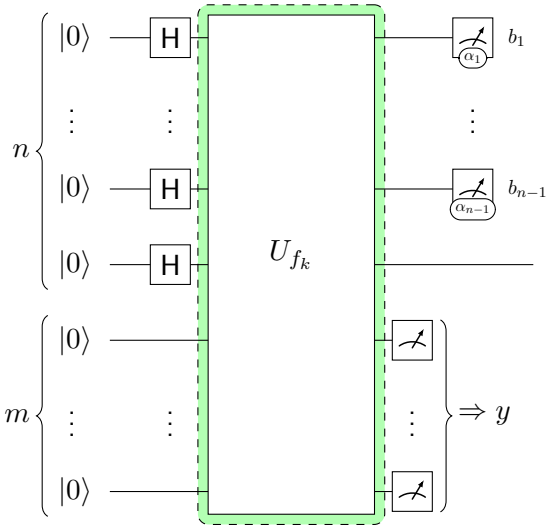


$t_k, k$



$$(\alpha_i \stackrel{s}{\leftarrow} \{0, \frac{\pi}{4} \dots \frac{7\pi}{4}\}_{i=1}^{n-1})$$

$k, (\alpha_i)$



$$|0\rangle^{\otimes n} |0\rangle^{\otimes m} \Rightarrow \sum_x |x\rangle |0\rangle^{\otimes m} \Rightarrow \sum_x |x\rangle |f_k(x)\rangle = \sum_y (|x\rangle + |x'\rangle) \otimes |y\rangle \Rightarrow (|x\rangle + |x'\rangle) \otimes |y\rangle$$



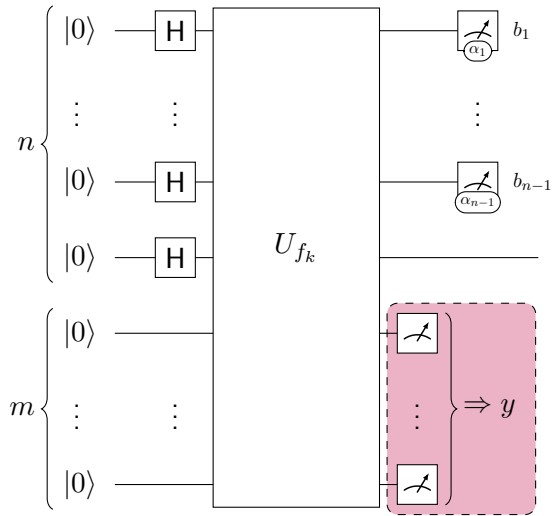
$t_k, k$



$$(\alpha_i \xleftarrow{\$} \{0, \frac{\pi}{4} \dots \frac{7\pi}{4}\}_{i=1}^{n-1})$$

$k, (\alpha_i)$

Compute circuit



$$|0\rangle^{\otimes n}|0\rangle^{\otimes m} \Rightarrow \sum_x |x\rangle|0\rangle^{\otimes m} \Rightarrow \sum_x |x\rangle|f_k(x)\rangle = \sum_y (|x\rangle + |x'\rangle) \otimes |y\rangle \Rightarrow (|x\rangle + |x'\rangle) \otimes |y\rangle \Rightarrow (\bigotimes_i |b_i\rangle) \otimes |+\theta\rangle \otimes |y\rangle$$



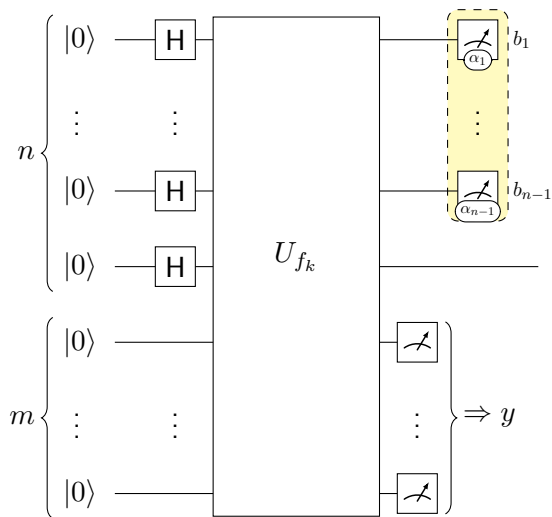
$t_k, k$



$$(\alpha_i \xleftarrow{s} \{0, \frac{\pi}{4} \dots \frac{7\pi}{4}\})_{i=1}^{n-1}$$

$k, (\alpha_i)$

Compute circuit



$$|0\rangle^{\otimes n} |0\rangle^{\otimes m} \Rightarrow \sum_x |x\rangle |0\rangle^{\otimes m} \Rightarrow \sum_x |x\rangle |f_k(x)\rangle = \sum_y (|x\rangle + |x'\rangle) \otimes |y\rangle \Rightarrow (|x\rangle + |x'\rangle) \otimes |y\rangle \Rightarrow (\bigotimes_i |b_i\rangle) \otimes |+\theta\rangle \otimes |y\rangle$$



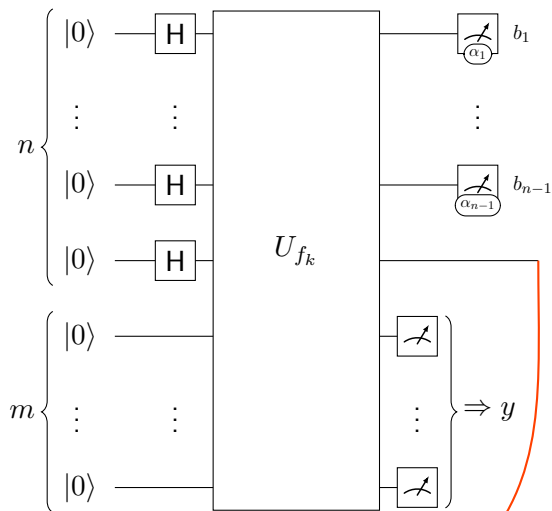
$t_k, k$



$$(\alpha_i \xleftarrow{\$} \{0, \frac{\pi}{4} \dots \frac{7\pi}{4}\})_{i=1}^{n-1}$$

$k, (\alpha_i)$

Compute circuit



$\Rightarrow$  Produces  $|+\theta\rangle$

$$|0\rangle^{\otimes n} |0\rangle^{\otimes m} \Rightarrow \sum_x |x\rangle |0\rangle^{\otimes m} \Rightarrow \sum_x |x\rangle |f_k(x)\rangle = \sum_y (|x\rangle + |x'\rangle) \otimes |y\rangle \Rightarrow (|x\rangle + |x'\rangle) \otimes |y\rangle \Rightarrow (\bigotimes_i |b_i\rangle) \otimes |+\theta\rangle \otimes |y\rangle$$



$t_k, k$

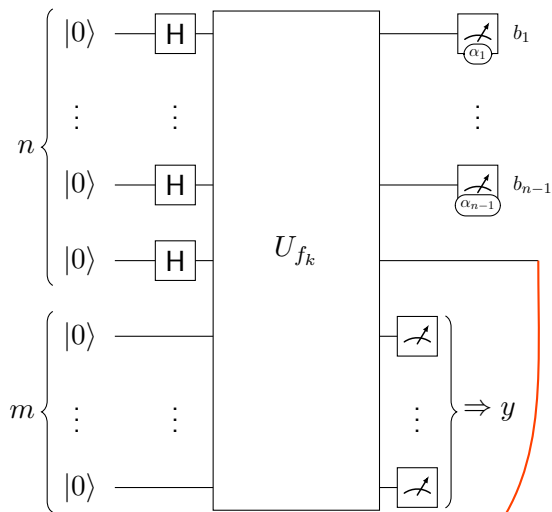


$$(\alpha_i \xleftarrow{\$} \{0, \frac{\pi}{4} \dots \frac{7\pi}{4}\}_{i=1}^{n-1})$$

$k, (\alpha_i)$

Compute circuit

$y, (b_i)$



$\Rightarrow$  Produces  $|+\theta\rangle$

$$|0\rangle^{\otimes n}|0\rangle^{\otimes m} \Rightarrow \sum_x |x\rangle|0\rangle^{\otimes m} \Rightarrow \sum_x |x\rangle|f_k(x)\rangle = \sum_y (|x\rangle + |x'\rangle) \otimes |y\rangle \Rightarrow (|x\rangle + |x'\rangle) \otimes |y\rangle \Rightarrow (\bigotimes_i |b_i\rangle) \otimes |+\theta\rangle \otimes |y\rangle$$



$t_k, k$



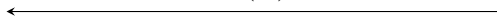
$$(\alpha_i \xleftarrow{\$} \{0, \frac{\pi}{4} \dots \frac{7\pi}{4}\}_{i=1}^{n-1})$$

$k, (\alpha_i)$

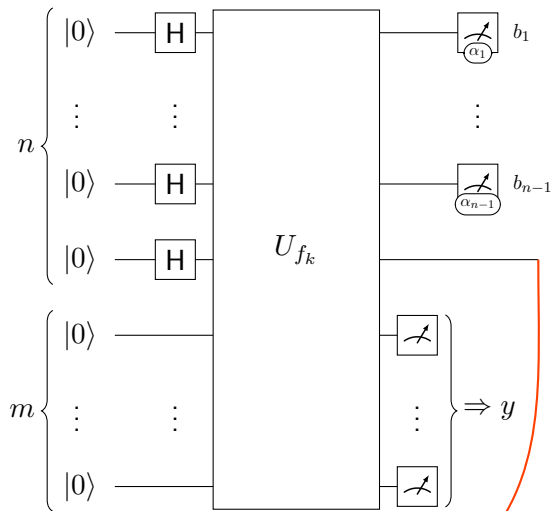


Compute circuit

$y, (b_i)$



$$(x, x') := \text{Inv}(t_k, y)$$



$\Rightarrow$  Produces  $|+\theta\rangle$

$$|0\rangle^{\otimes n} |0\rangle^{\otimes m} \Rightarrow \sum_x |x\rangle |0\rangle^{\otimes m} \Rightarrow \sum_x |x\rangle |f_k(x)\rangle = \sum_y (|x\rangle + |x'\rangle) \otimes |y\rangle \Rightarrow (|x\rangle + |x'\rangle) \otimes |y\rangle \Rightarrow (\bigotimes_i |b_i\rangle) \otimes |+\theta\rangle \otimes |y\rangle$$



$t_k, k$



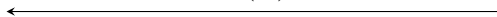
$$(\alpha_i \xleftarrow{\$} \{0, \frac{\pi}{4} \dots \frac{7\pi}{4}\}_{i=1}^{n-1})$$

$k, (\alpha_i)$



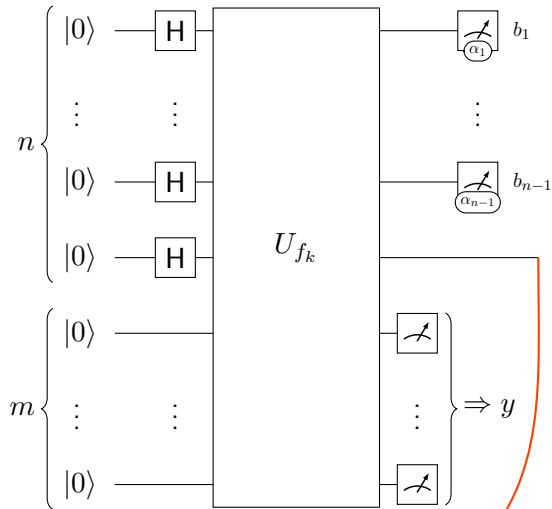
Compute circuit

$y, (b_i)$



$$(x, x') := \text{Inv}(t_k, y)$$

$$\theta := (-1)^{x_n} \sum_{i=1}^{n-1} (x_i - x'_i)(b_i\pi + \alpha_i)$$



$\Rightarrow$  Produces  $|+\theta\rangle$

$$|0\rangle^{\otimes n} |0\rangle^{\otimes m} \Rightarrow \sum_x |x\rangle |0\rangle^{\otimes m} \Rightarrow \sum_x |x\rangle |f_k(x)\rangle = \sum_y (|x\rangle + |x'\rangle) \otimes |y\rangle \Rightarrow (|x\rangle + |x'\rangle) \otimes |y\rangle \Rightarrow (\bigotimes_i |b_i\rangle) \otimes |+\theta\rangle \otimes |y\rangle$$



$t_k, k$



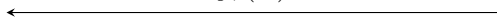
$$(\alpha_i \xleftarrow{\$} \{0, \frac{\pi}{4} \dots \frac{7\pi}{4}\})_{i=1}^{n-1}$$

$k, (\alpha_i)$



Compute circuit

$y, (b_i)$



$$(x, x') := \text{Inv}(t_k, y)$$

$$\theta := (-1)^{x_n} \sum_{i=1}^{n-1} (x_i - x'_i)(b_i \pi + \alpha_i)$$

