t_k, k

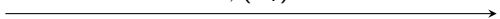
t_k, k

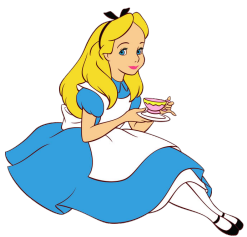
$(\alpha_i \xleftarrow{\$} \{0, \frac{\pi}{4} \dots \frac{7\pi}{4}\})_{i=1}^{n-1}$

t_k, k

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

$k, (\alpha_i)$



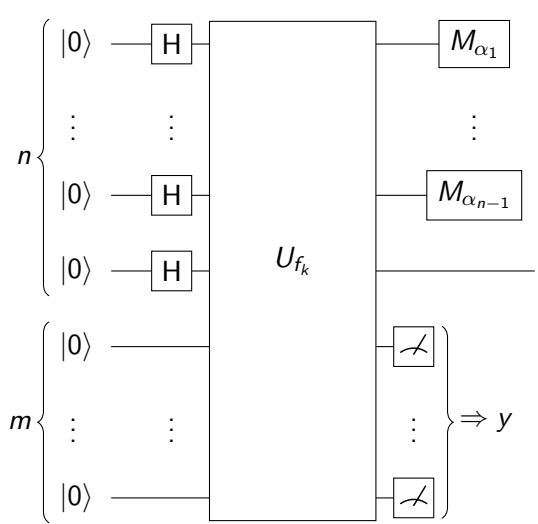


t_k, k

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

$k, (\alpha_i)$

Compute circuit

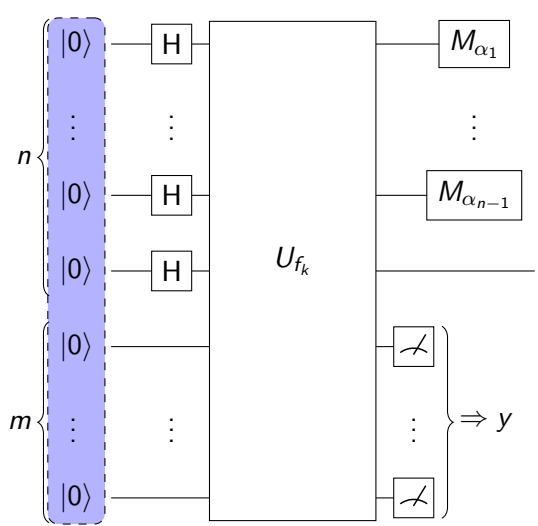


t_k, k

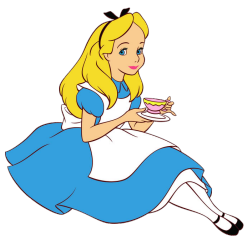
$(\alpha_i \xleftarrow{\$} \{0, \frac{\pi}{4} \dots \frac{7\pi}{4}\})_{i=1}^{n-1}$

$k, (\alpha_i)$

Compute circuit



$|0\rangle|0\rangle$

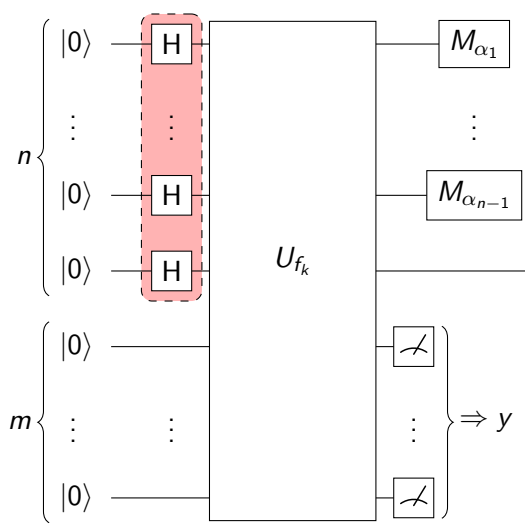


t_k, k

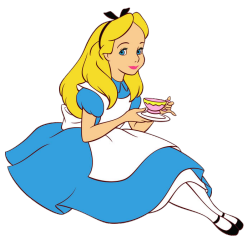
$(\alpha_i \xleftarrow{\$} \{0, \frac{\pi}{4} \ldots \frac{7\pi}{4}\})_{i=1}^{n-1}$

$k, (\alpha_i)$

Compute circuit



$|0\rangle|0\rangle \Rightarrow \sum_x |x\rangle|0\rangle$

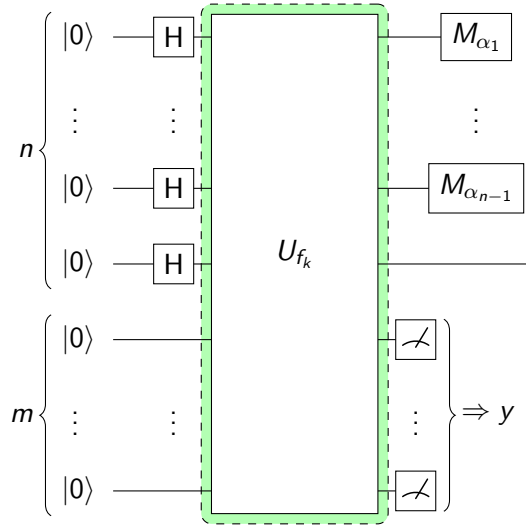


t_k, k

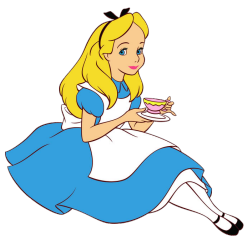
$(\alpha_i \xleftarrow{\$} \{0, \frac{\pi}{4} \dots \frac{7\pi}{4}\})_{i=1}^{n-1}$

$k, (\alpha_i)$

Compute circuit



$|0\rangle|0\rangle \Rightarrow \sum_x |x\rangle|0\rangle \Rightarrow \sum_x |x\rangle|f_k(x)\rangle$

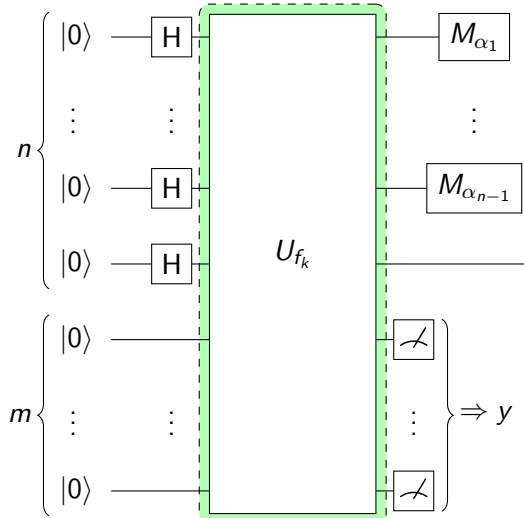


t_k, k

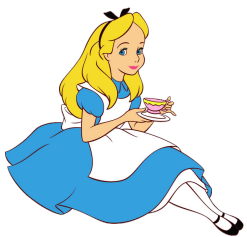
$(\alpha_i \xleftarrow{\$} \{0, \frac{\pi}{4} \dots \frac{7\pi}{4}\})_{i=1}^{n-1}$

$k, (\alpha_i)$

Compute circuit



$|0\rangle|0\rangle \Rightarrow \sum_x |x\rangle|0\rangle \Rightarrow \sum_x |x\rangle|f_k(x)\rangle = \sum_y (|x\rangle + |x'\rangle) \otimes |y\rangle$

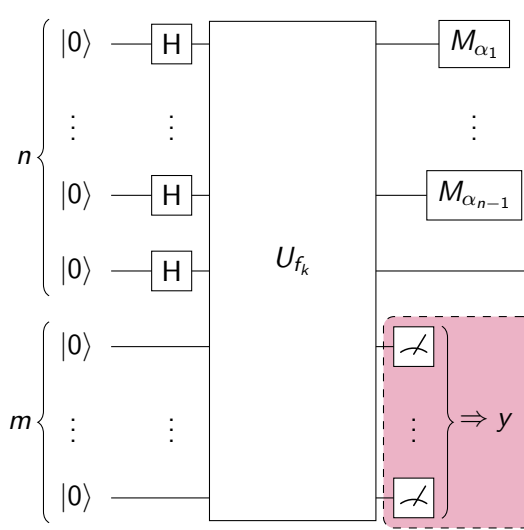


t_k, k

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

$k, (\alpha_i)$

Compute circuit



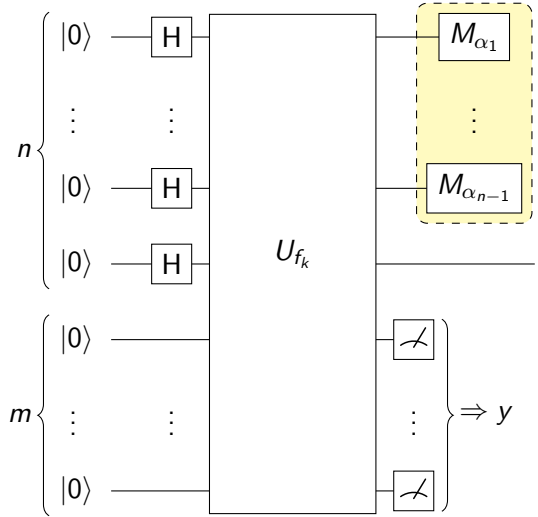
$|0\rangle|0\rangle \Rightarrow \sum_x |x\rangle|0\rangle \Rightarrow \sum_x |x\rangle|f_k(x)\rangle = \sum_y (|x\rangle + |x'\rangle) \otimes |y\rangle \Rightarrow (|x\rangle + |x'\rangle) \otimes |y\rangle$

t_k, k

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

$k, (\alpha_i)$

Compute circuit



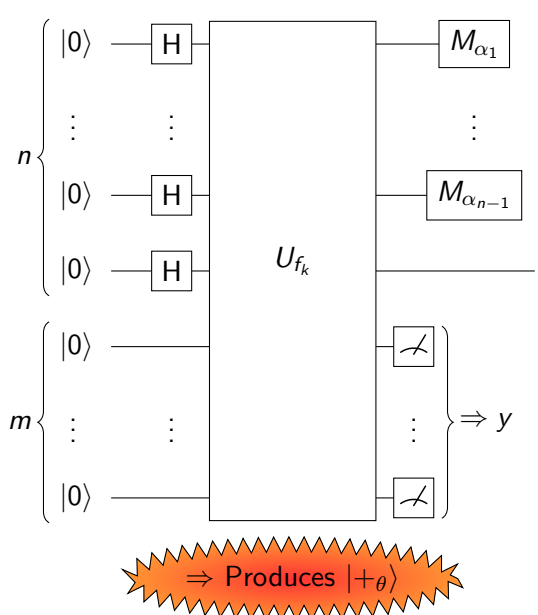
$|0\rangle|0\rangle \Rightarrow \sum_x |x\rangle|0\rangle \Rightarrow \sum_x |x\rangle|f_k(x)\rangle = \sum_y (|x\rangle + |x'\rangle) \otimes |y\rangle \Rightarrow (|x\rangle + |x'\rangle) \otimes |y\rangle \Rightarrow (\bigotimes_i |b_i\rangle) \otimes |+_\theta\rangle \otimes |y\rangle$

t_k, k

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

$k, (\alpha_i)$

Compute circuit



$$|0\rangle|0\rangle \Rightarrow \sum_x |x\rangle|0\rangle \Rightarrow \sum_x |x\rangle|f_k(x)\rangle = \sum_y (|x\rangle + |x'\rangle) \otimes |y\rangle \Rightarrow (|x\rangle + |x'\rangle) \otimes |y\rangle \Rightarrow (\bigotimes_i |b_i\rangle) \otimes |+_\theta\rangle \otimes |y\rangle$$

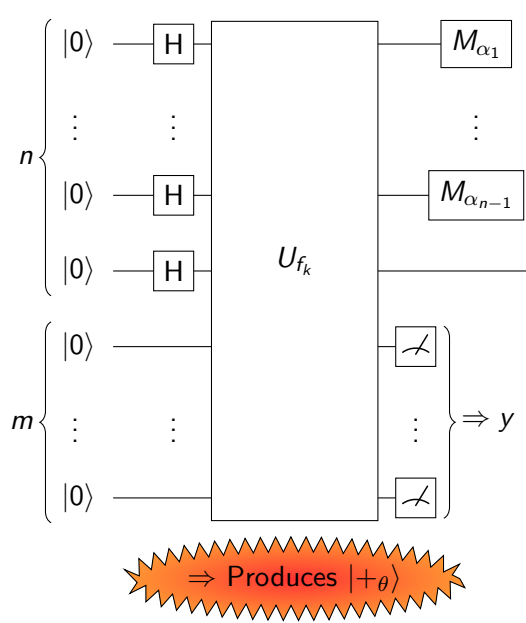
t_k, k

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

$k, (\alpha_i)$ →

Compute circuit

← $y, (b_i)$



$|0\rangle|0\rangle \Rightarrow \sum_x |x\rangle|0\rangle \Rightarrow \sum_x |x\rangle|f_k(x)\rangle = \sum_y (|x\rangle + |x'\rangle) \otimes |y\rangle \Rightarrow (|x\rangle + |x'\rangle) \otimes |y\rangle \Rightarrow (\bigotimes_i |b_i\rangle) \otimes |+_\theta\rangle \otimes |y\rangle$

t_k, k

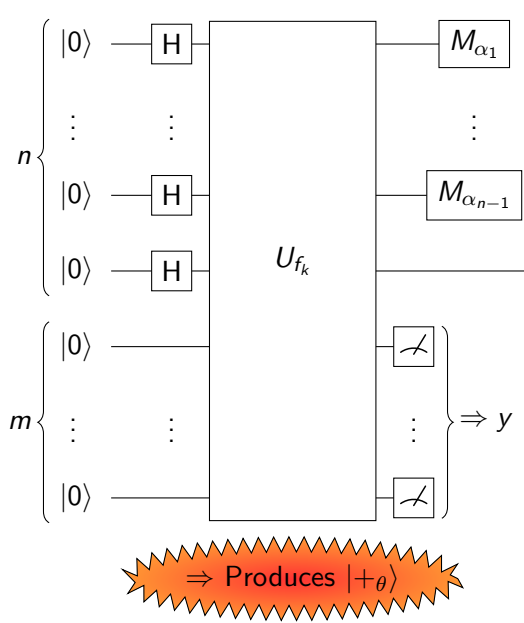
$(\alpha_i \xleftarrow{\$} \{0, \frac{\pi}{4} \dots \frac{7\pi}{4}\})_{i=1}^{n-1}$

$k, (\alpha_i)$

Compute circuit

$y, (b_i)$

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



$|0\rangle|0\rangle \Rightarrow \sum_x |x\rangle|0\rangle \Rightarrow \sum_x |x\rangle|f_k(x)\rangle = \sum_y (|x\rangle + |x'\rangle) \otimes |y\rangle \Rightarrow (|x\rangle + |x'\rangle) \otimes |y\rangle \Rightarrow (\bigotimes_i |b_i\rangle) \otimes |+_\theta\rangle \otimes |y\rangle$

t_k, k

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

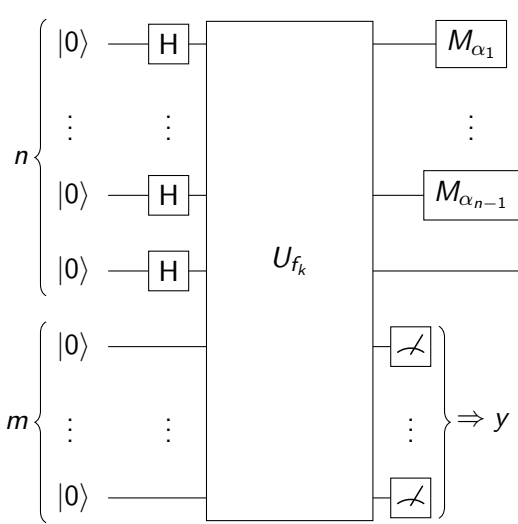
$k, (\alpha_i)$ →

Compute circuit

← $y, (b_i)$

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

$\theta := \frac{\pi}{4}(-1)^{x_n} \sum_{i=1}^{n-1}(x_i - x'_i)(4b_i + \alpha_i)$



$|0\rangle|0\rangle \Rightarrow \sum_x |x\rangle|0\rangle \Rightarrow \sum_x |x\rangle|f_k(x)\rangle = \sum_y (|x\rangle + |x'\rangle) \otimes |y\rangle \Rightarrow (|x\rangle + |x'\rangle) \otimes |y\rangle \Rightarrow (\bigotimes_i |b_i\rangle) \otimes |+_\theta\rangle \otimes |y\rangle$

t_k, k

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

$k, (\alpha_i)$

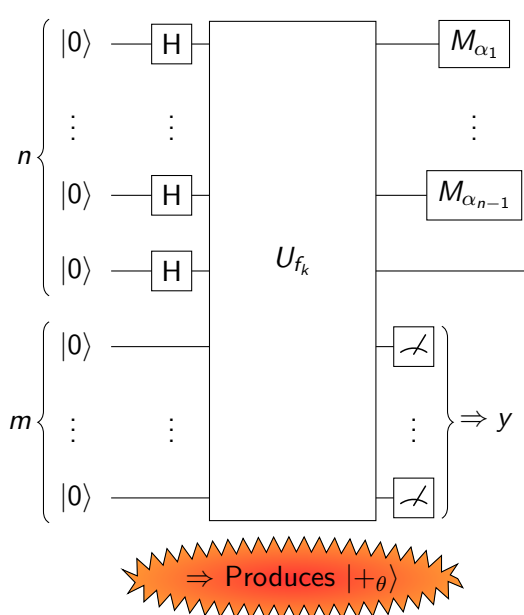
⇒ Gets θ

Compute circuit

$y, (b_i)$

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

$\theta := \frac{\pi}{4}(-1)^{x_n} \sum_{i=1}^{n-1}(x_i - x'_i)(4b_i + \alpha_i)$



$|0\rangle|0\rangle \Rightarrow \sum_x |x\rangle|0\rangle \Rightarrow \sum_x |x\rangle|f_k(x)\rangle = \sum_y (|x\rangle + |x'\rangle) \otimes |y\rangle \Rightarrow (|x\rangle + |x'\rangle) \otimes |y\rangle \Rightarrow (\bigotimes_i |b_i\rangle) \otimes |+_\theta\rangle \otimes |y\rangle$