

## One-way

This function is hard to invert...

## 2-Regular

2 preimages for all elements in  $Im(f_k)$

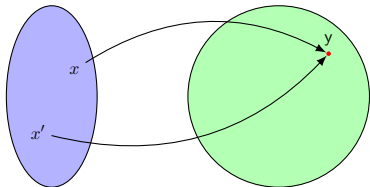
Functions  $\{f_k\}$

## Trapdoor

... except if you have the trapdoor  $t_k$  associated to the function index  $k$ .

## Collision resistant

Without trapdoor  $t_k$ , hard to find  $x \neq x'$  such that  $f_k(x) = f_k(x')$



## One-way

This function is hard to invert...

## 2-Regular

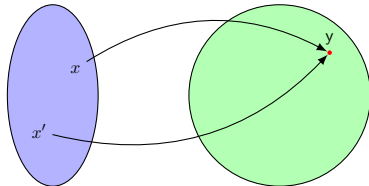
2 preimages for all elements in  $Im(f_k)$

Functions  $\{f_k\}$

$\Rightarrow$  Candidate based on [MP11]

## Trapdoor

... except if you have the trapdoor  $t_k$  associated to the function index  $k$ .



## Collision resistant

Without trapdoor  $t_k$ , hard to find  $x \neq x'$  such that  $f_k(x) = f_k(x')$