



Brute-force hash function

## **CR - Collision Resistance**

➡ given  $H$ , hard to find  $m$  and  $m'$  such that  $H(m) = H(m') = x$

Given a hash function  $H$  of  $n$  bits output

- Reaching all possibilities
- On average, an attacker should try half of them

m



X

2n cases

2n-1 cases



Brute-forcing a hash function



## CR - Collision Resistance

➡ given  $H$ , hard to find  $m$  and  $m'$  such that  $H(m) = H(m') = x$

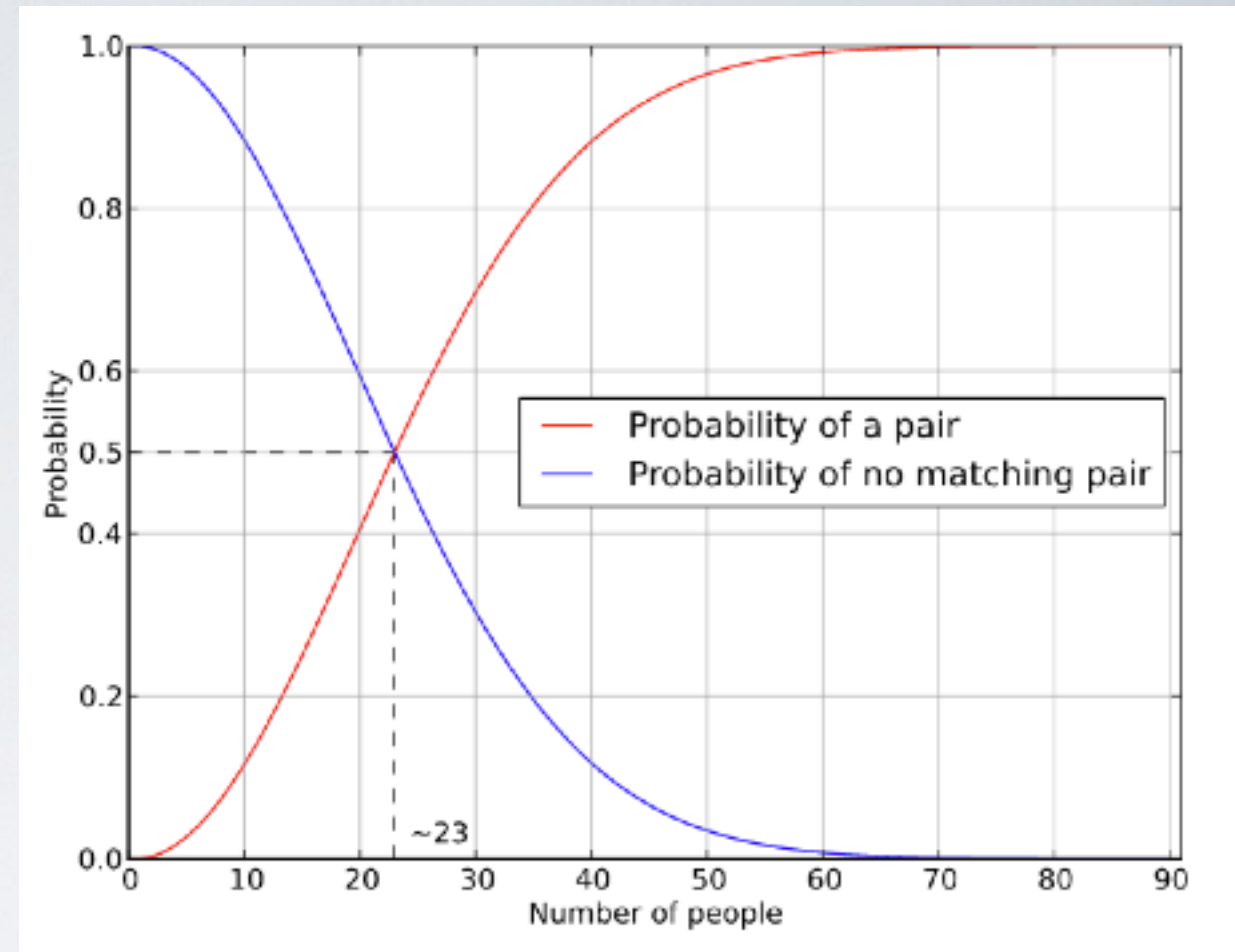
Given a hash function  $H$  of  $n$  bits output

- Reaching all possibilities  $2^n$  cases
- ~~• On average, an attacker should try half of them  $2^{n-1}$  cases~~



# Birthday Paradox

*“There are 50% chance that 2 people have the same birthday in a room of 23 people”*



## N-bits security

- ➡ Given a hash function **H** of **n** bits output, a collision can be found in around  **$2^{n/2}$**  evaluations  
e.g SHA-256 is 128 bits security