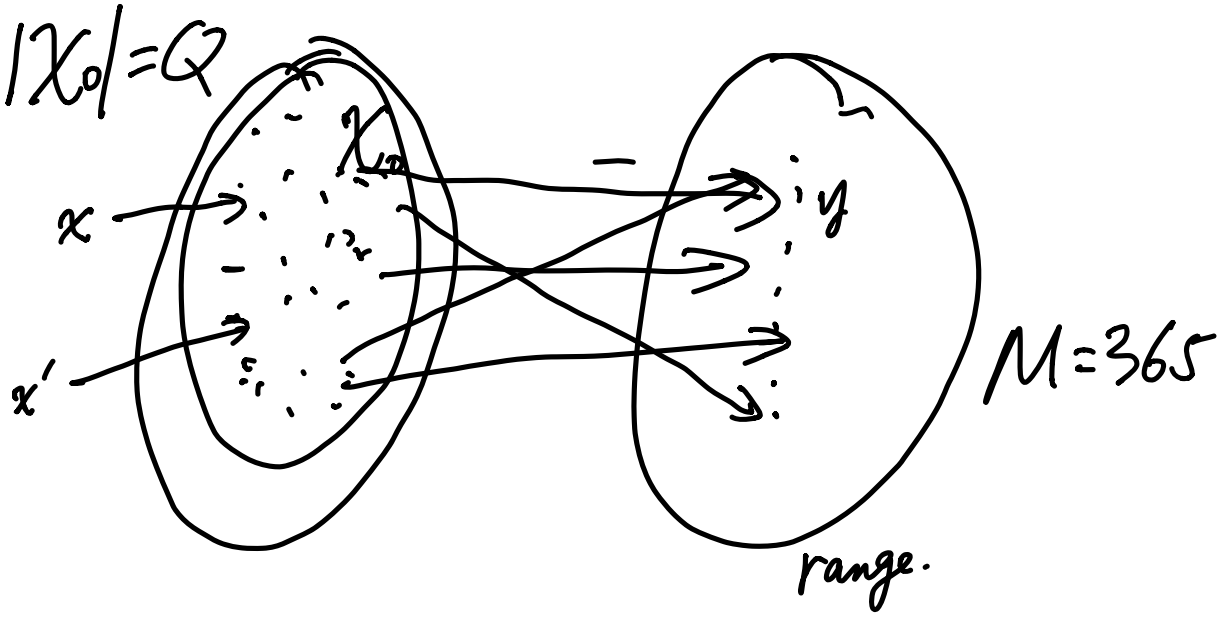
# ECE 471/571. Hash functions (cont'd)

## birthday paradox




hash : people → birthdays

Pr[ any person's birthday = one date from 1 ~ 365 ]

$= \frac{1}{365} = \frac{1}{M}$. (random oracle).

Pr[at least two people have same birthday]

① pick first person $d_1$.. $\Pr[d_2 \neq d_1]$

② ..... 2nd person $d_2$ $= 1 - \frac{1}{365}$

③ ..... 3rd person $d_3$ $= \frac{364}{365}$

$= [\ \frac{1}{}$

$\Pr[d_3 \neq d_1, d_3 \neq d_2] = 1 - \frac{2}{365} = 1 - \frac{1}{m}$

$\vdots$

(2) $\Pr[\text{bd of } i\text{-th person is different}] : 1 - \frac{i}{365}$

$\Pr[\text{None of } Q \text{ persons have same BD}]$

$$= \prod_{i=1}^{Q} \left(1 - \frac{i}{365}\right) = \prod_{i=1}^{Q} \left(1 - \frac{i}{m}\right)$$

$$\approx \prod_{i=1}^{Q} e^{-\frac{i}{m}} = e^{-\sum_{i=1}^{Q} \frac{i}{m}}$$

$$= e^{-\frac{Q(Q-1)}{2m}}$$

$$\simeq e^{-\frac{Q^2}{2m}}$$

$$1 - e^{-\frac{Q^2}{2m}} = \Pr[\text{at least 2 persons have same BD}]$$

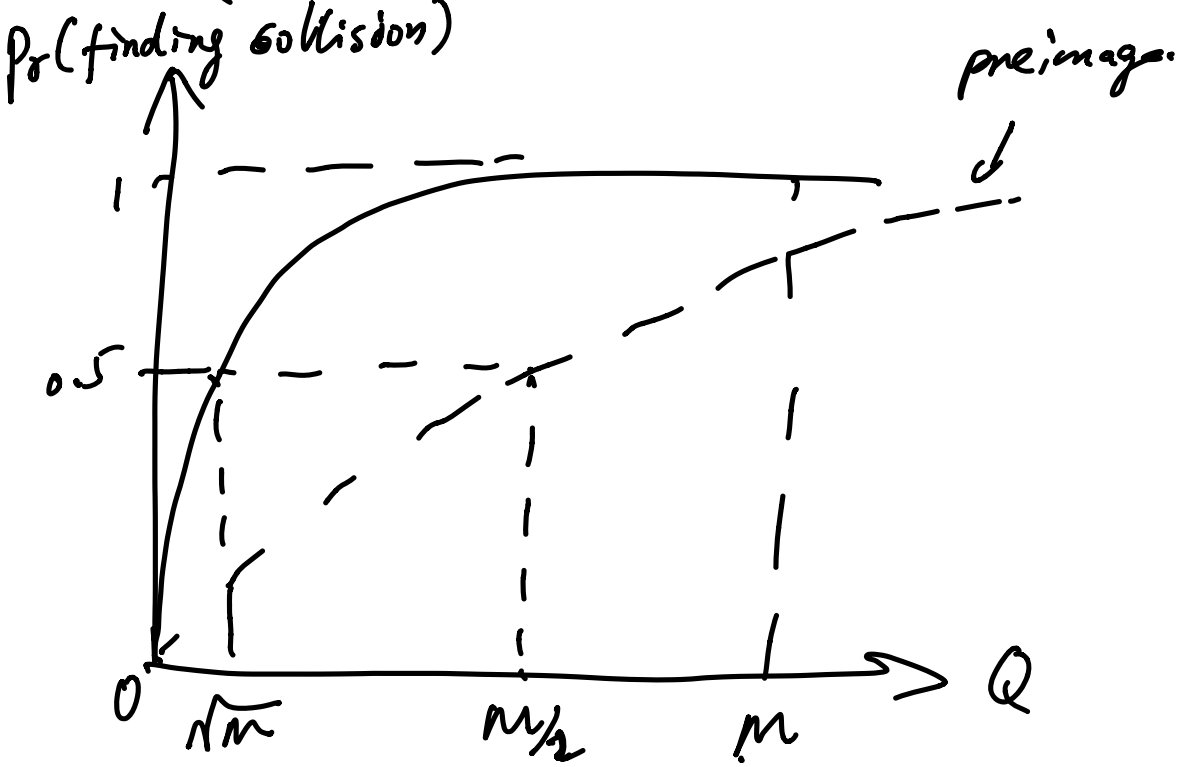
$\geq 0.5$

$$Q \geq \sqrt{2M \cdot \ln 2}$$

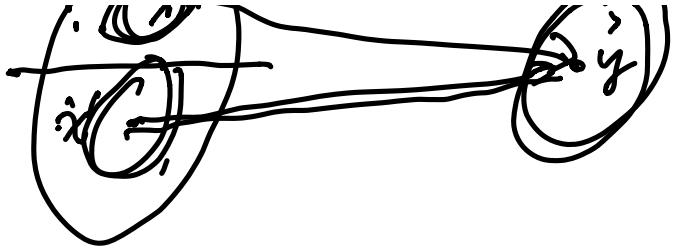
$$\approx 1.177\sqrt{M} \ll M$$

$M = 365$.

$Q \geq 1.177 \times \sqrt{365} \approx 23$




Collison resistance $\Rightarrow$ Second-preimage resistance.




collison resistance $\Rightarrow$ preimage resistance

when $|X| > 2 \cdot |Y|$