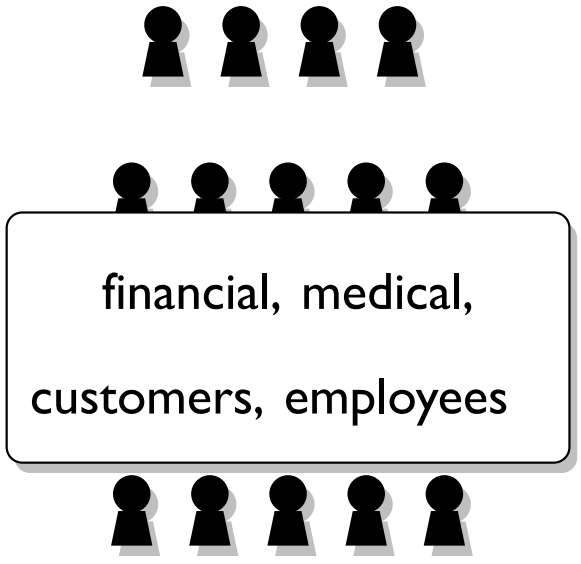
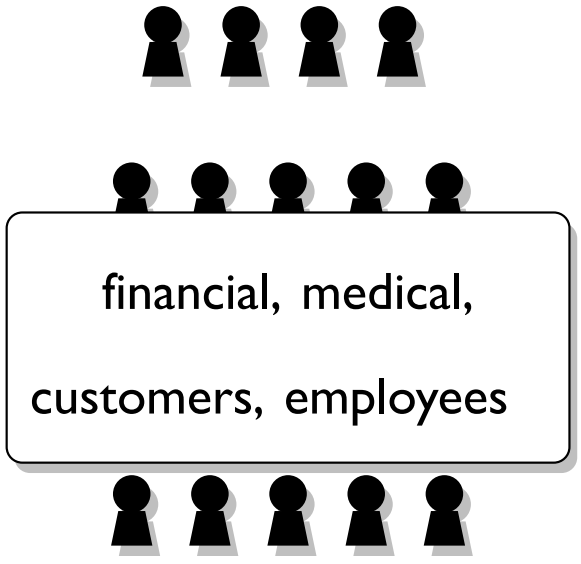
Cryptography, Encryption, *and* Big Data

Hoeteck Wee

ENS, Paris

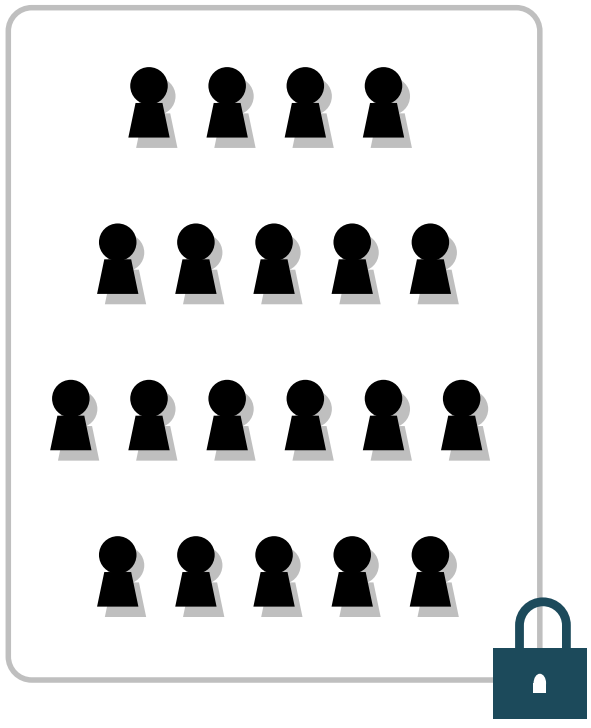


BIG DATA



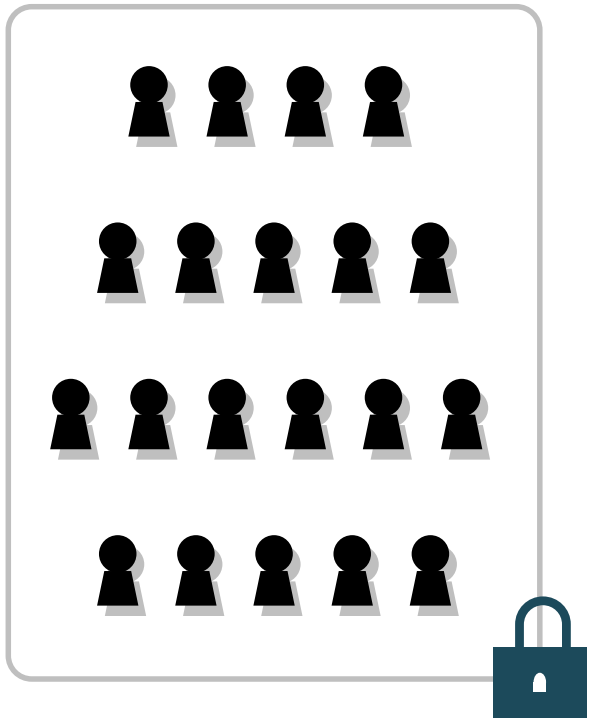
BIG DATA

Q. privacy?



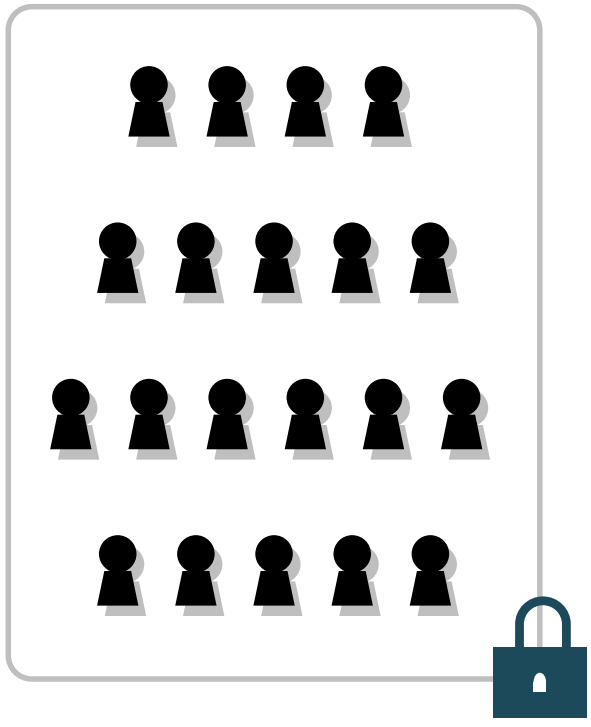
BIG DATA

Q. privacy?



BIG DATA

Q. utility + privacy?



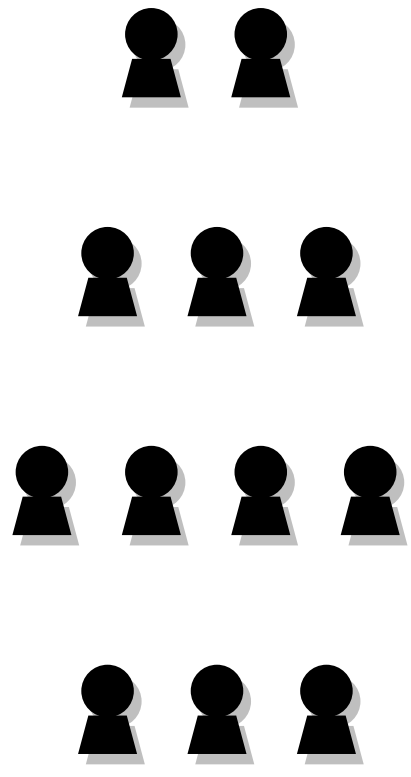
BIG DATA

Q. utility + privacy?

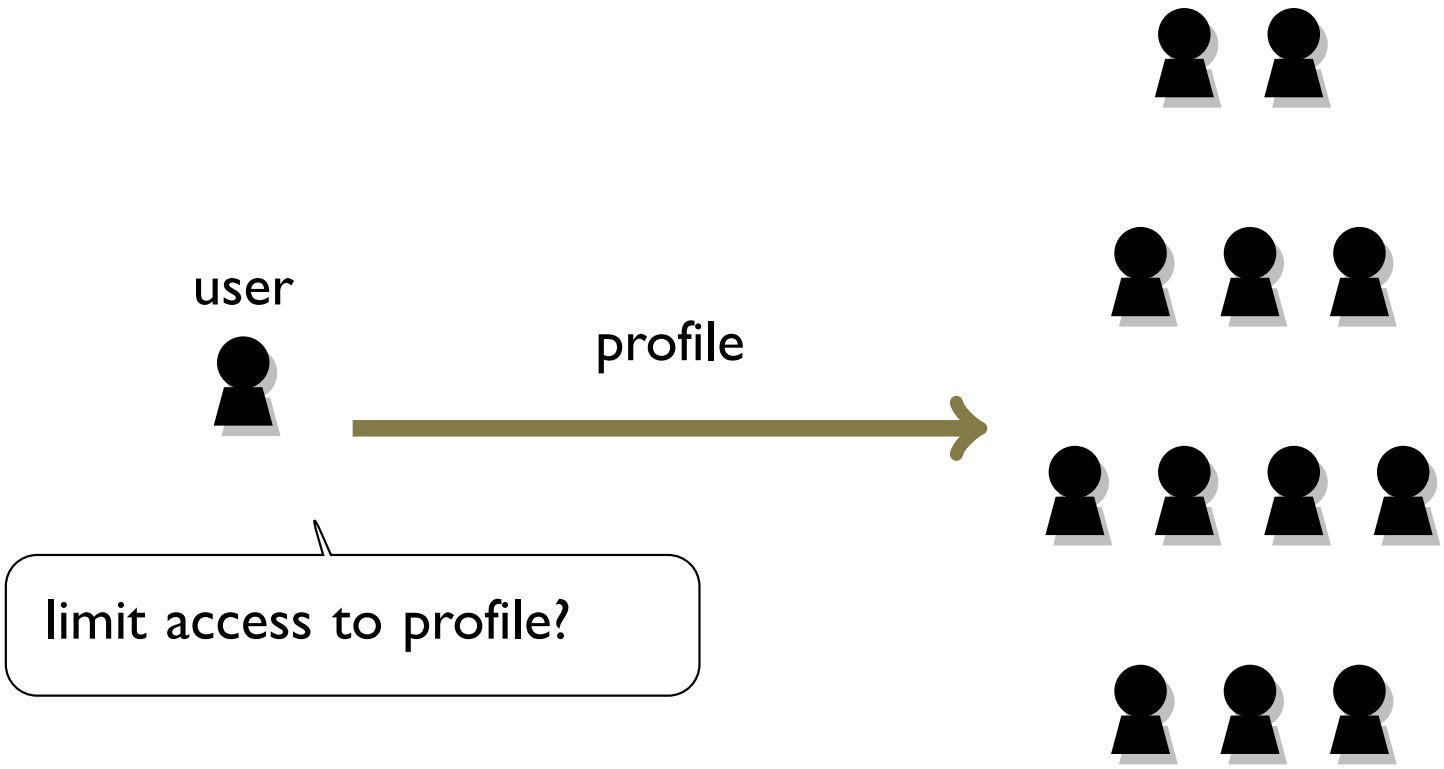
restrict **access** + **computation**

dating + big data

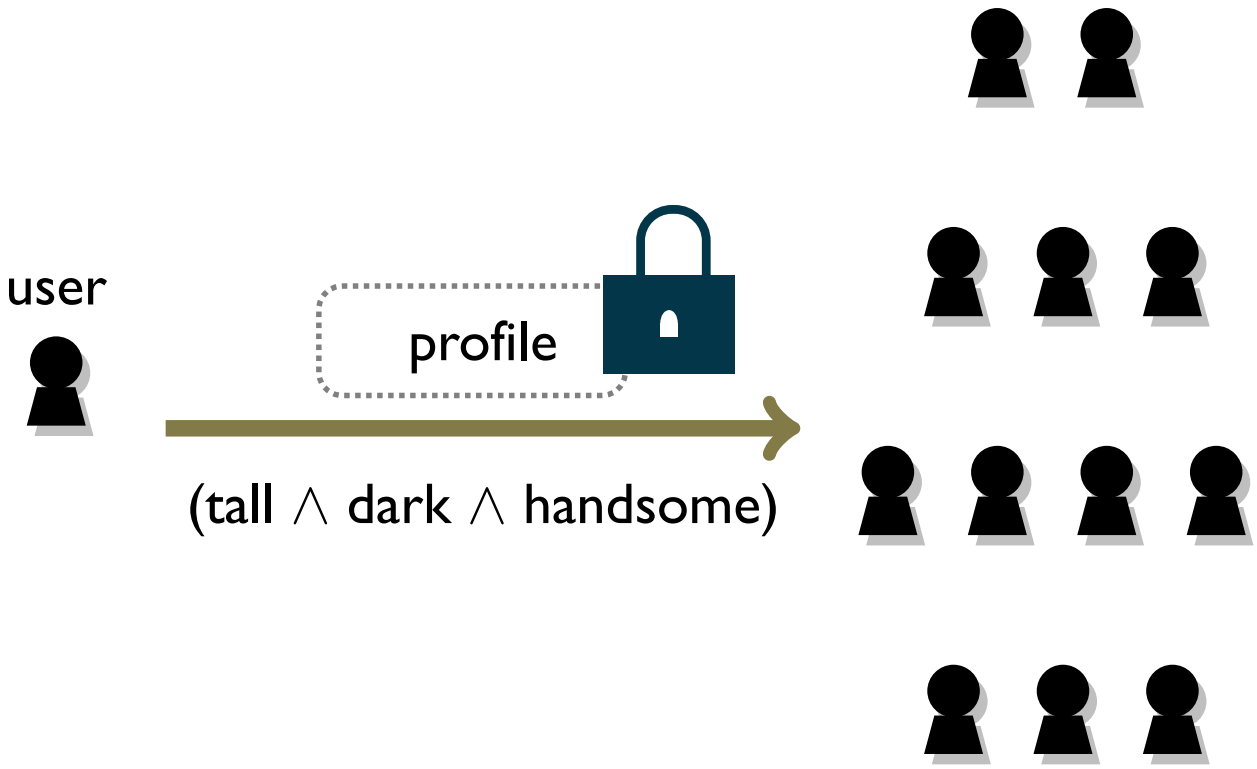
user



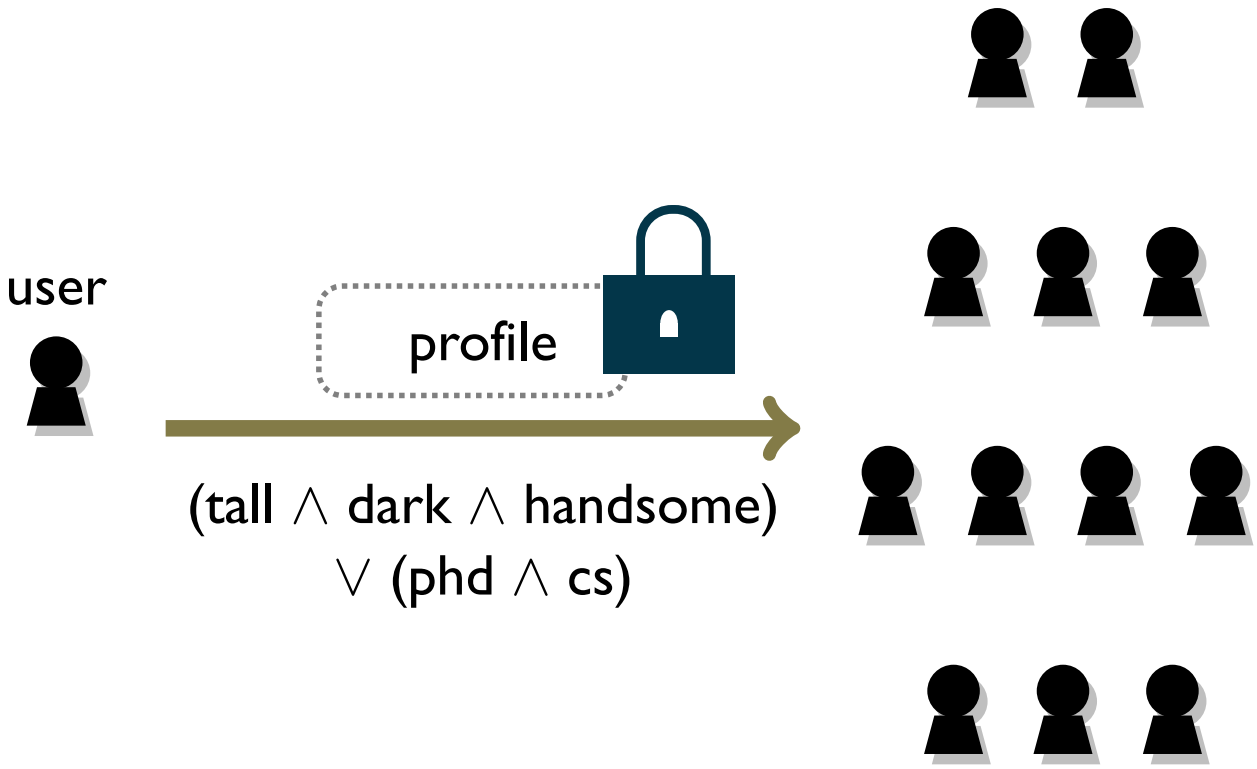
dating + big data



dating + big data



dating + big data



attribute-based encryption

$\text{cs} \wedge \text{phd}$

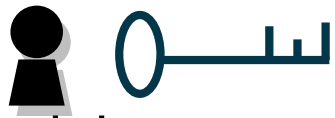
cs phd

cs msc

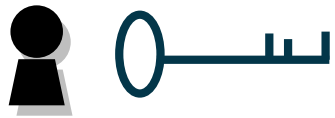
bio phd

attribute-based encryption

cs ∧ phd



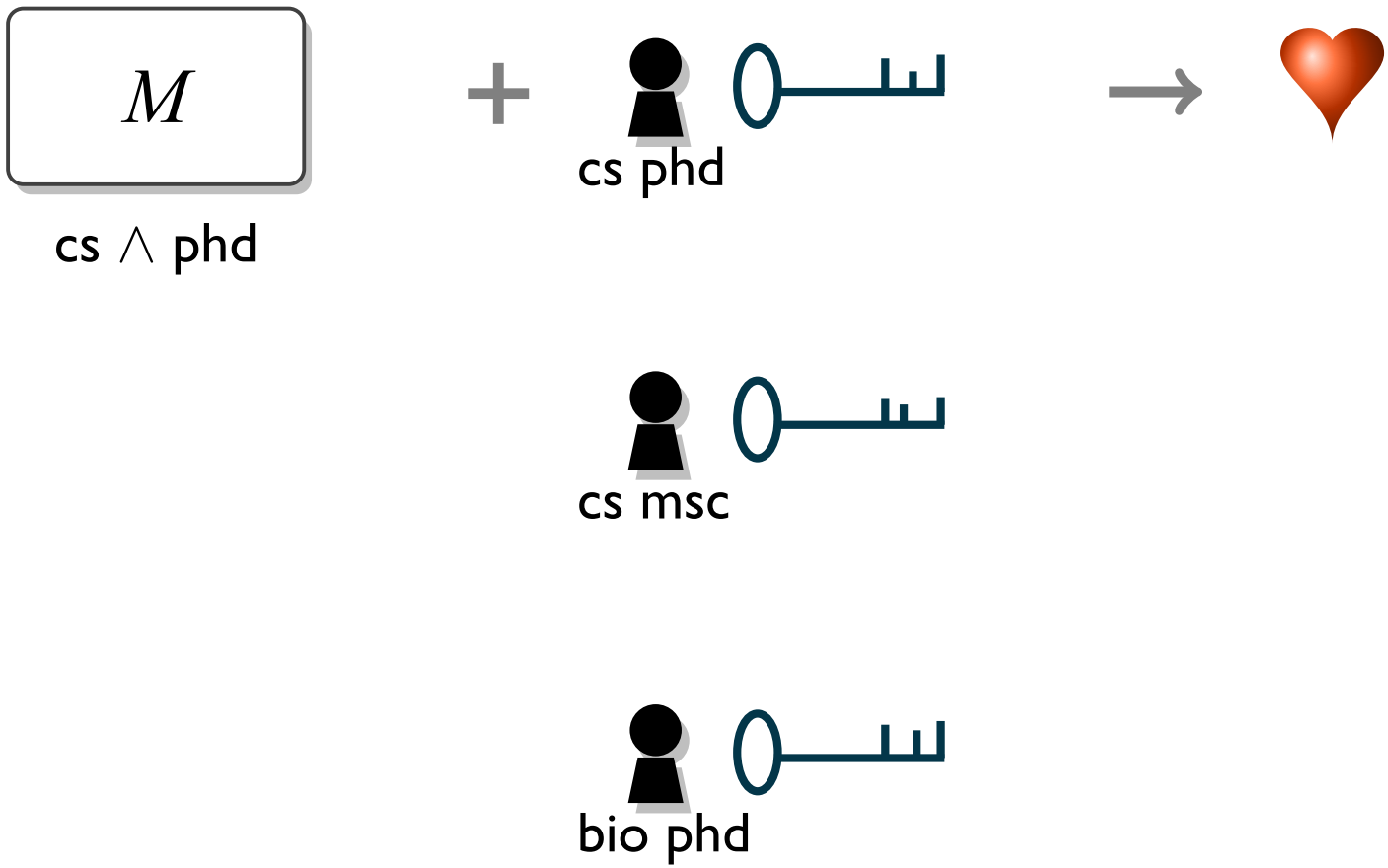
cs phd



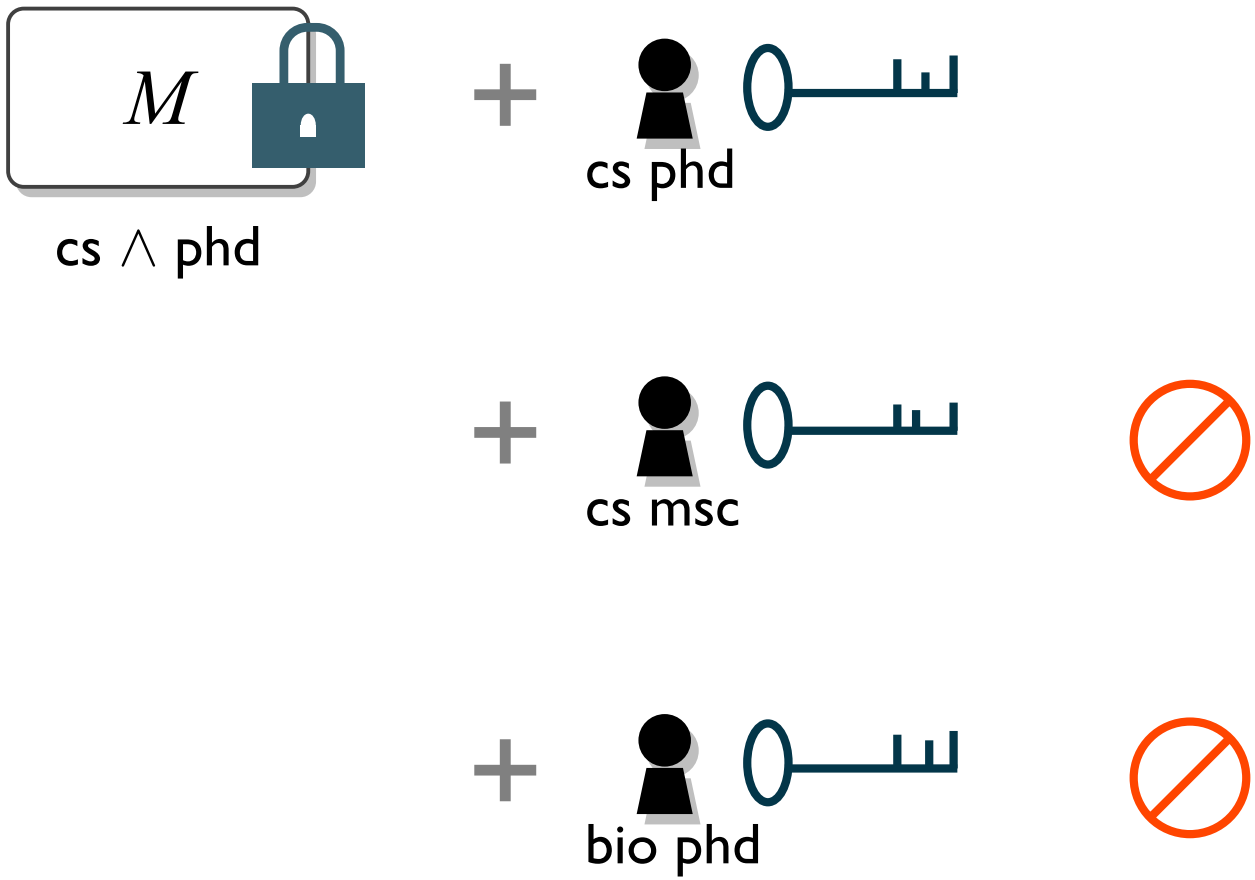
cs msc

bio phd

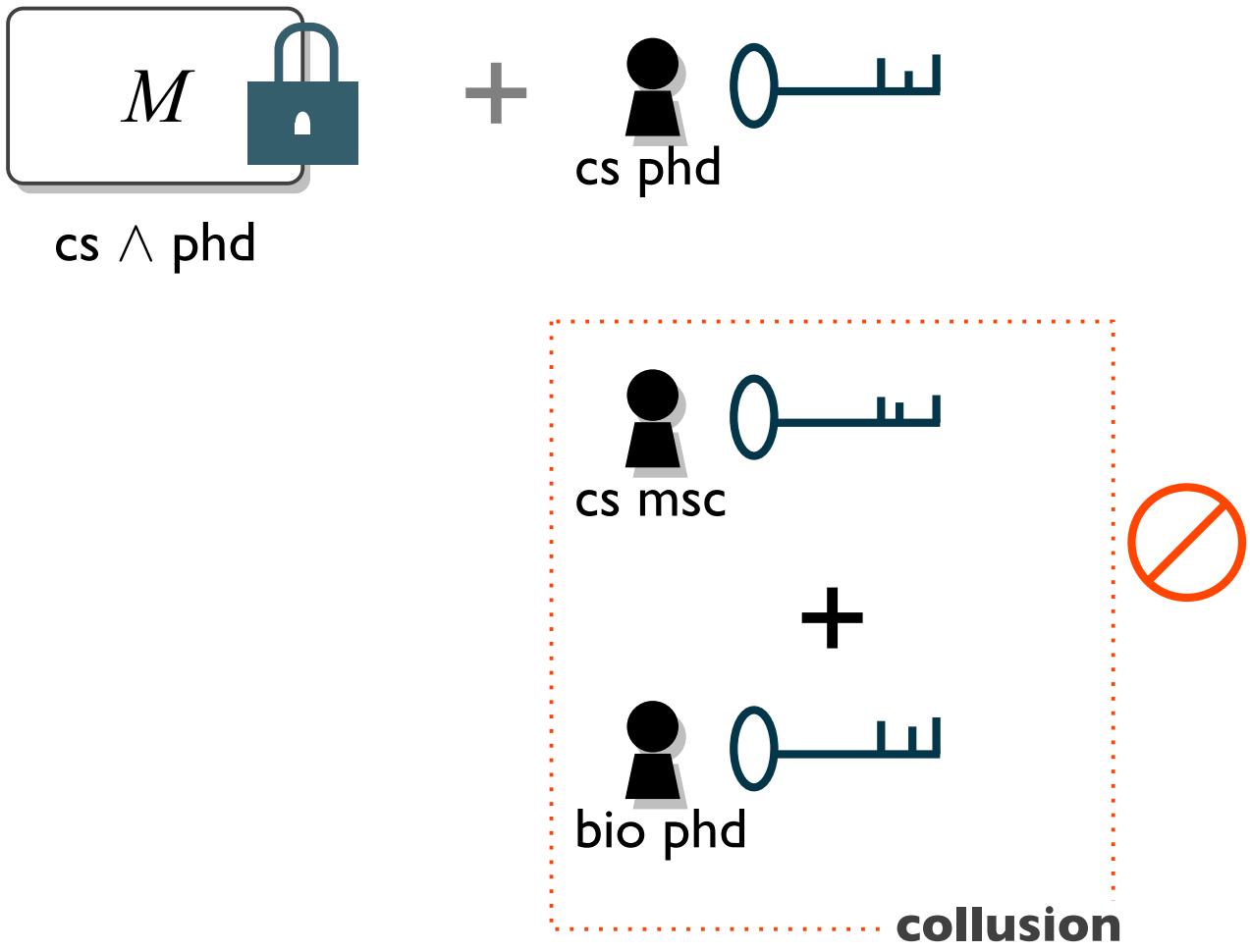
attribute-based encryption



attribute-based encryption

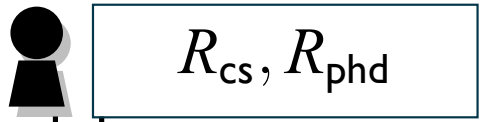


attribute-based encryption

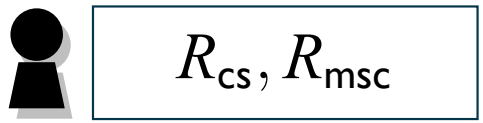


attribute-based encryption

cs $\wedge$ phd



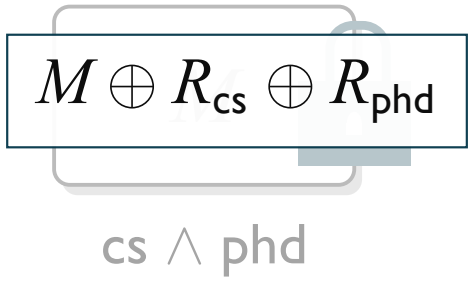
cs phd

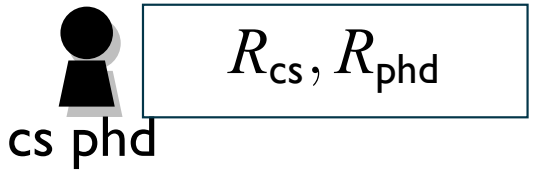


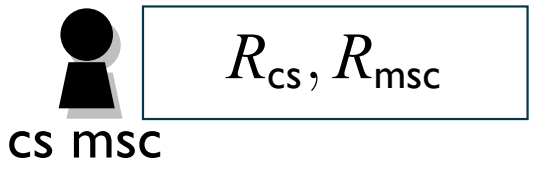
cs msc

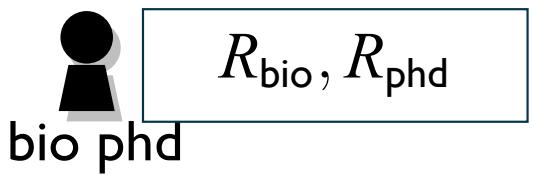
bio phd

attribute-based encryption

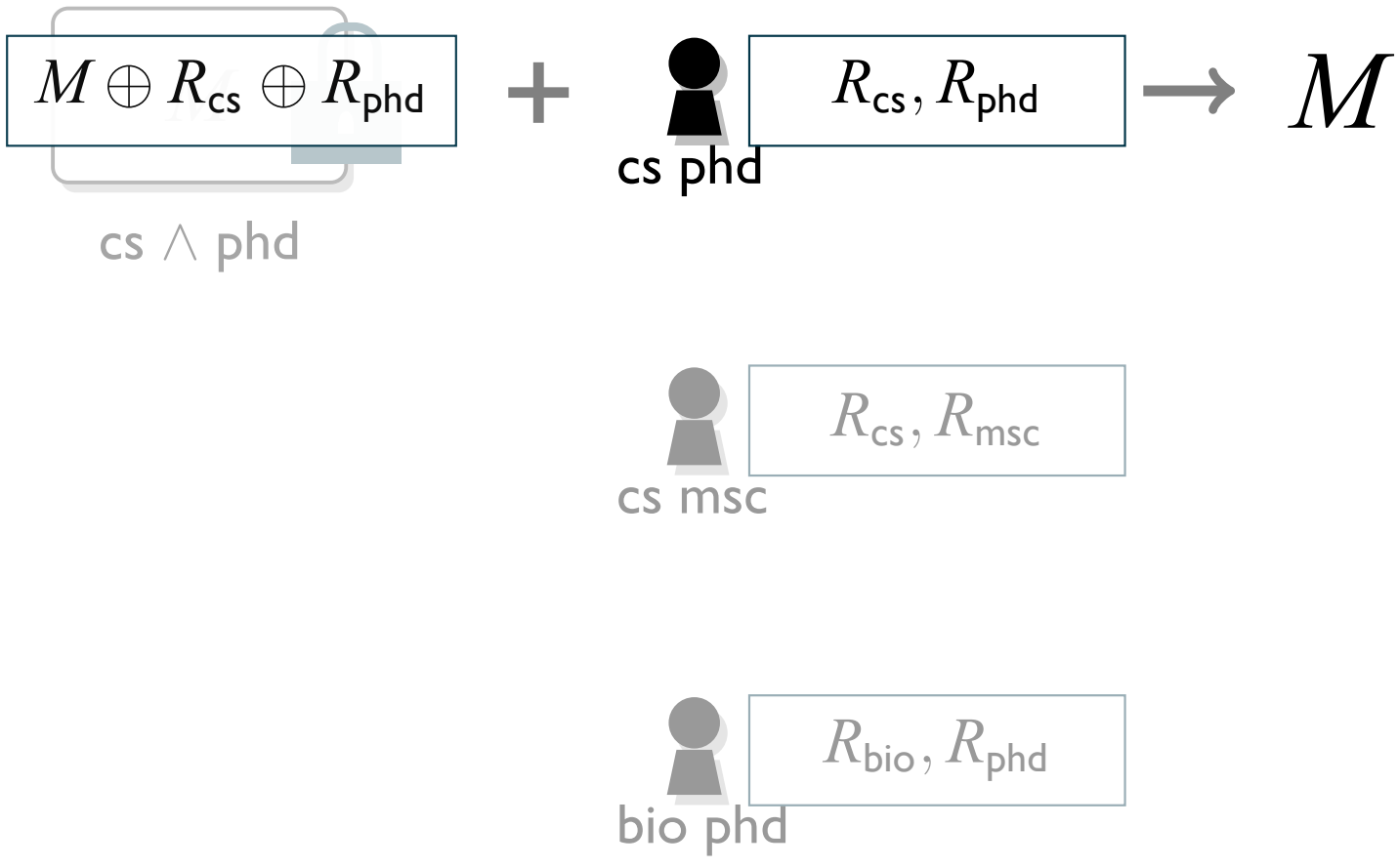






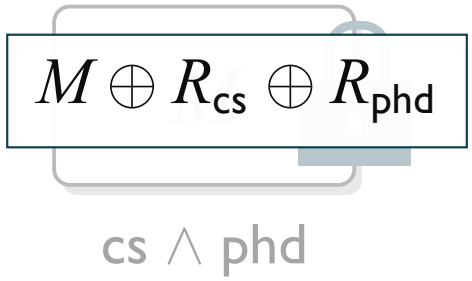


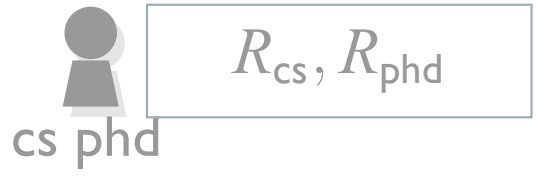
attribute-based encryption

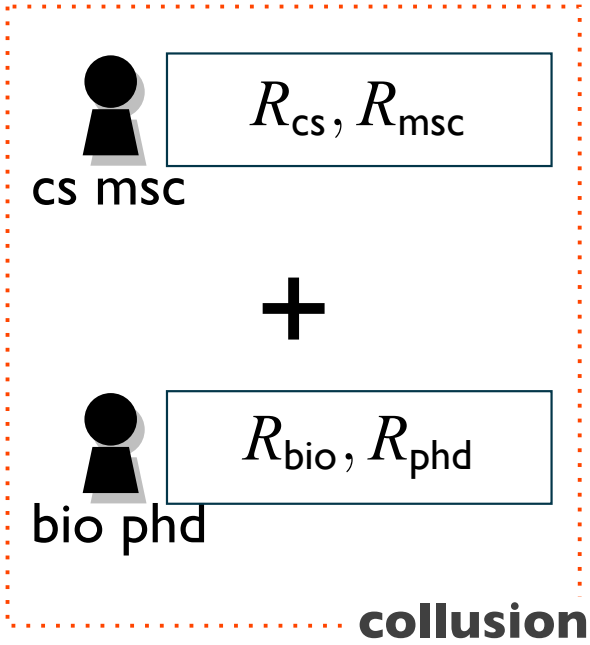


attribute-based encryption

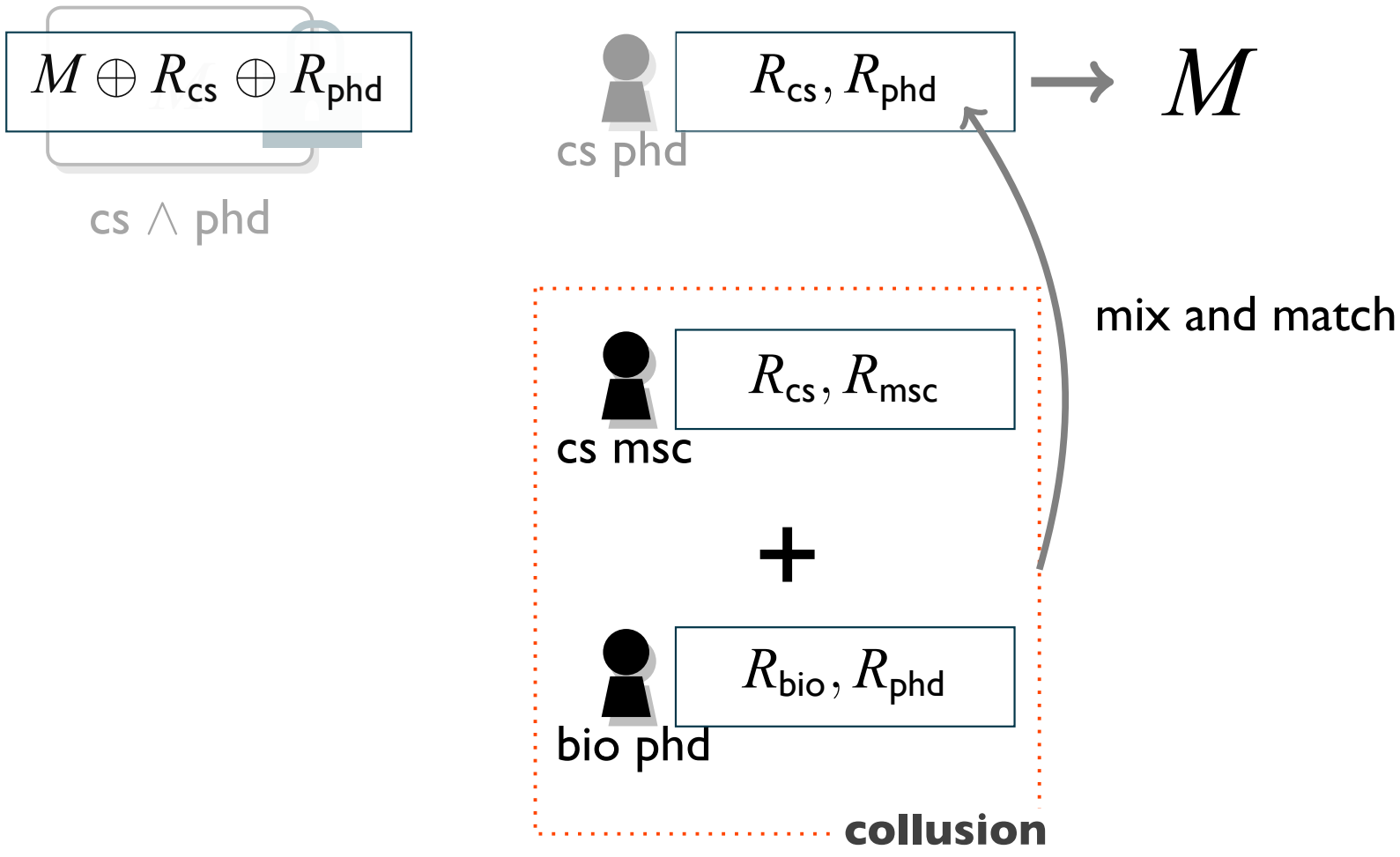
attribute-based encryption



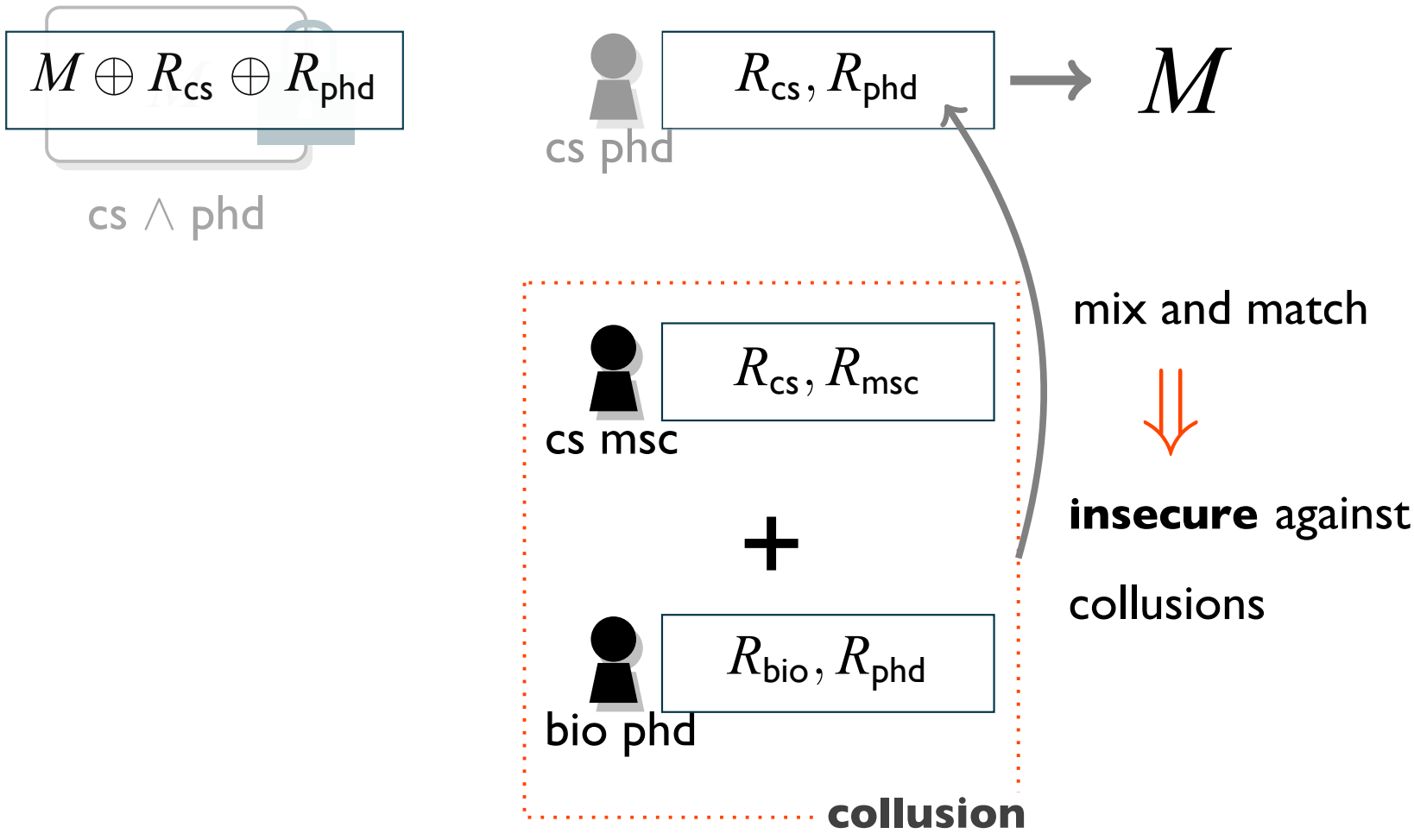




attribute-based encryption



attribute-based encryption



attribute-based encryption

[GVW13] ABE for circuits

strings $R \rightarrow$ functions $\phi(\cdot)$

one-use $\rightarrow$ many-use

$R_{\text{cs}}, R_{\text{phd}}$

$R_{\text{cs}}, R_{\text{msc}}$

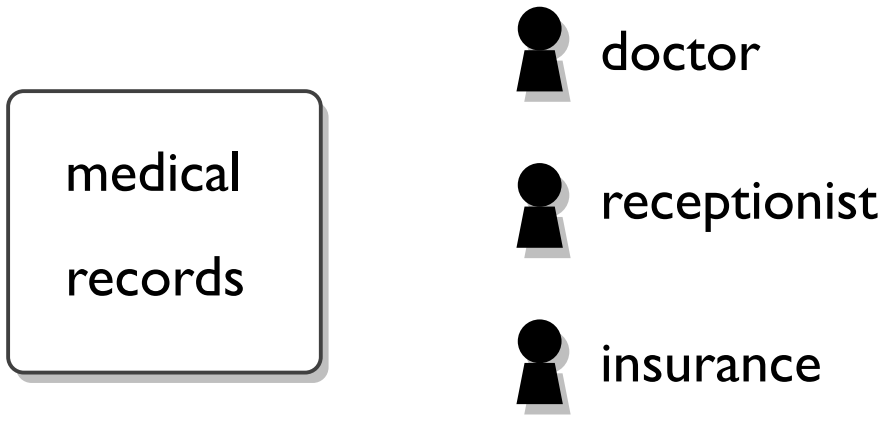
cs msc

$R_{\text{bio}}, R_{\text{phd}}$

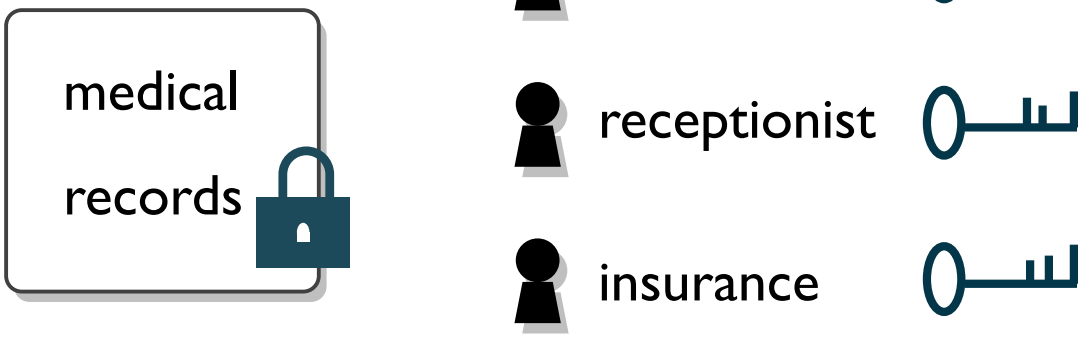
bio phd

mix and match

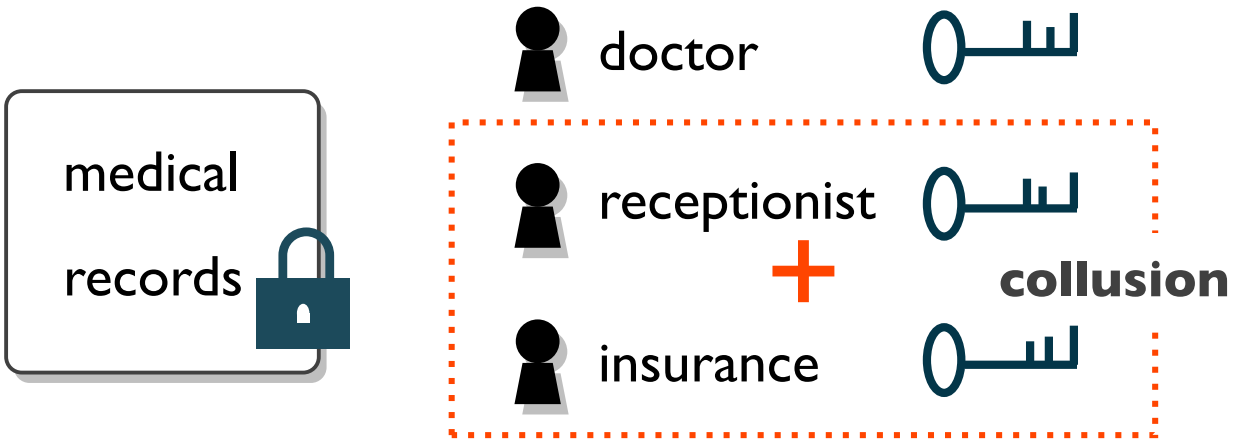
functional encryption [SW05, GPSW06, BSW11]



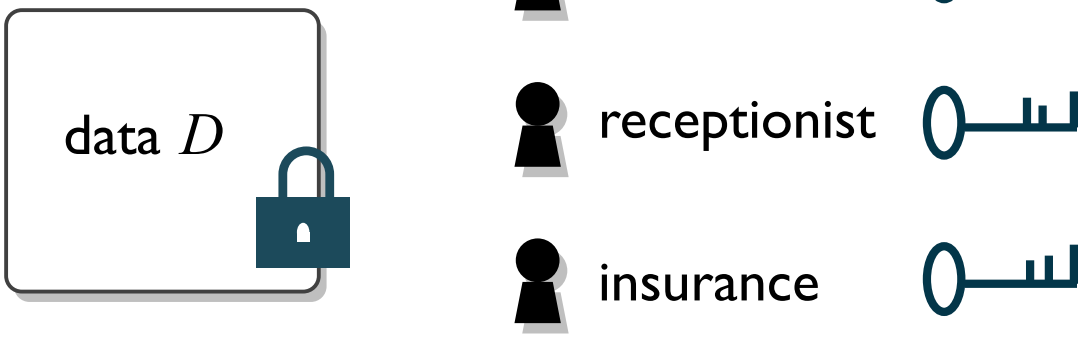
functional encryption [SW05, GPSW06, BSW11]



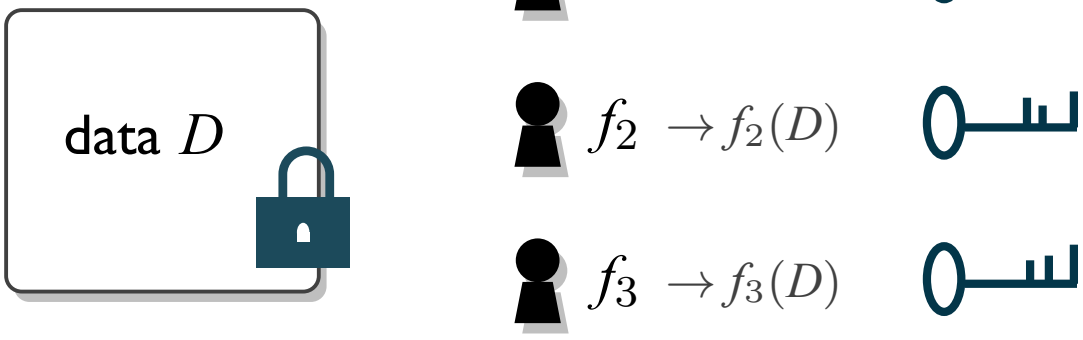
functional encryption [SW05, GPSW06, BSW11]



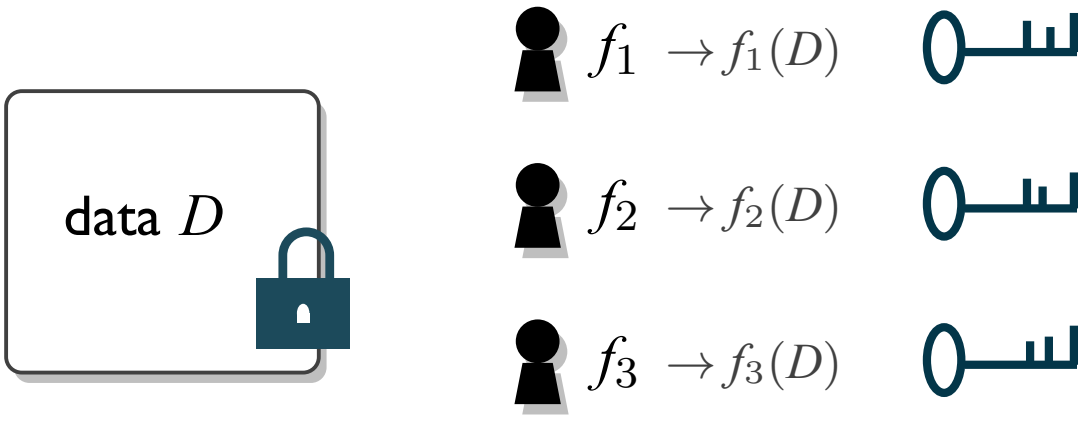
functional encryption [SW05, GPSW06, BSW11]



functional encryption [SW05, GPSW06, BSW11]



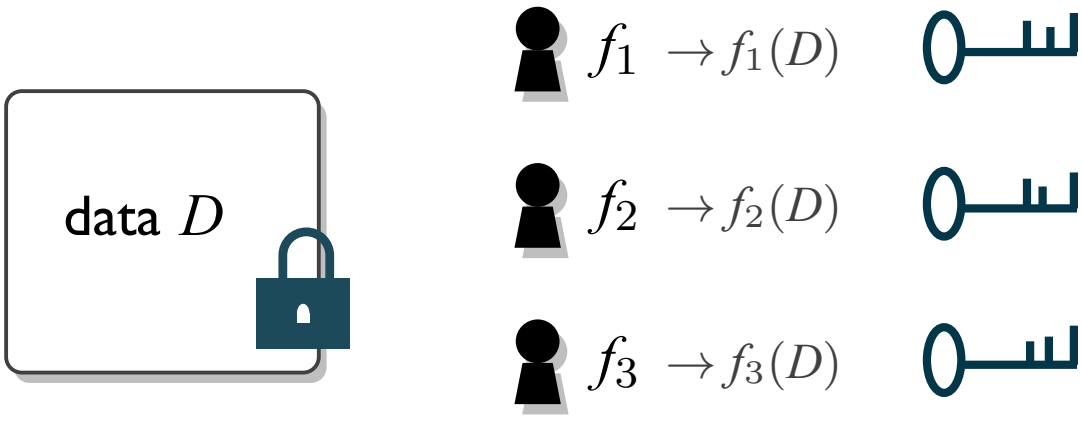
functional encryption [SW05, GPSW06, BSW11]



fully homomorphic encryption (FHE)

- encrypted answers
- unrestricted computation

functional encryption [SW05, GPSW06, BSW11]

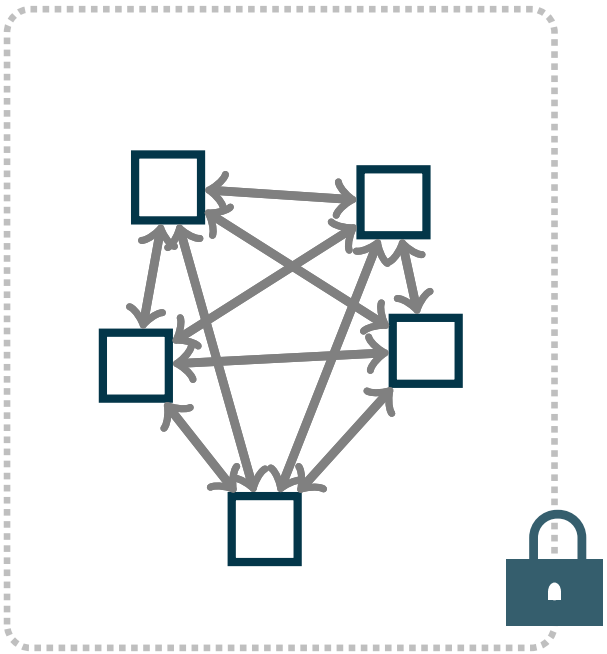


“ functional encryption for **all** functions? ”

my **research**

goal. advances in foundations of functional encryption

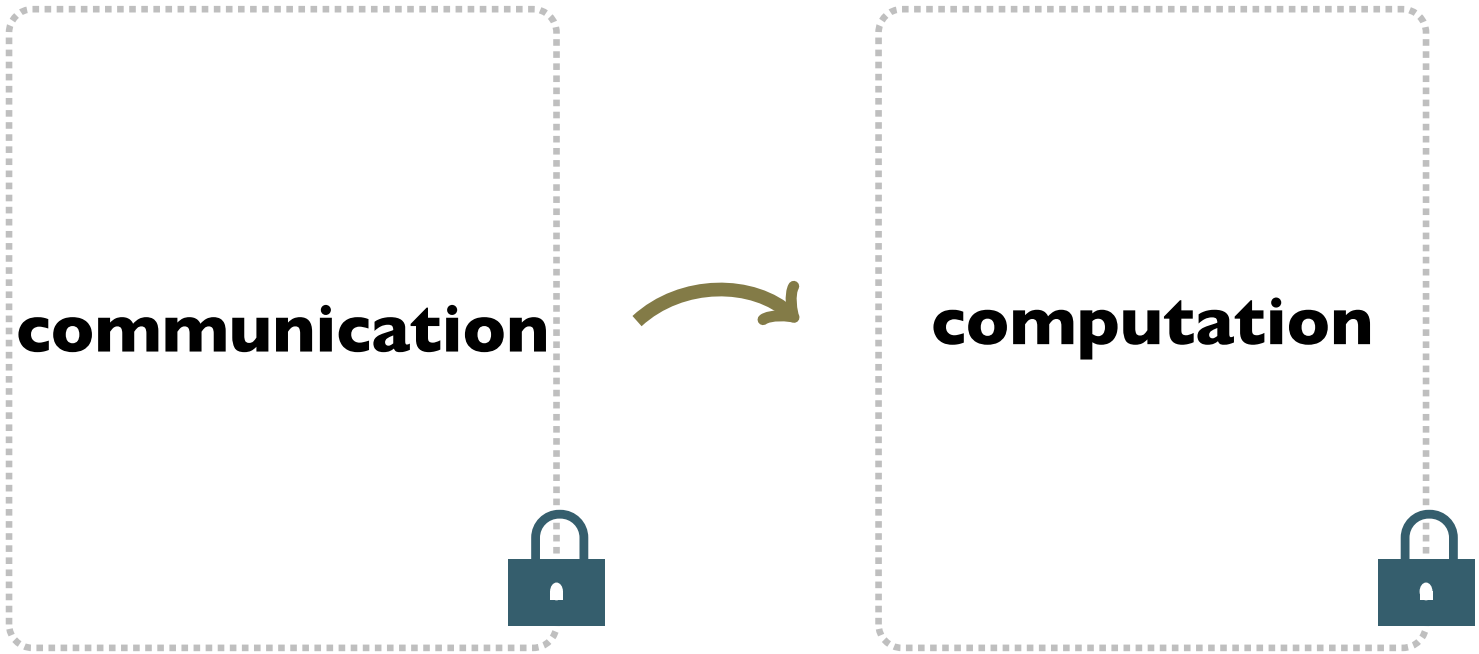
communication



internet

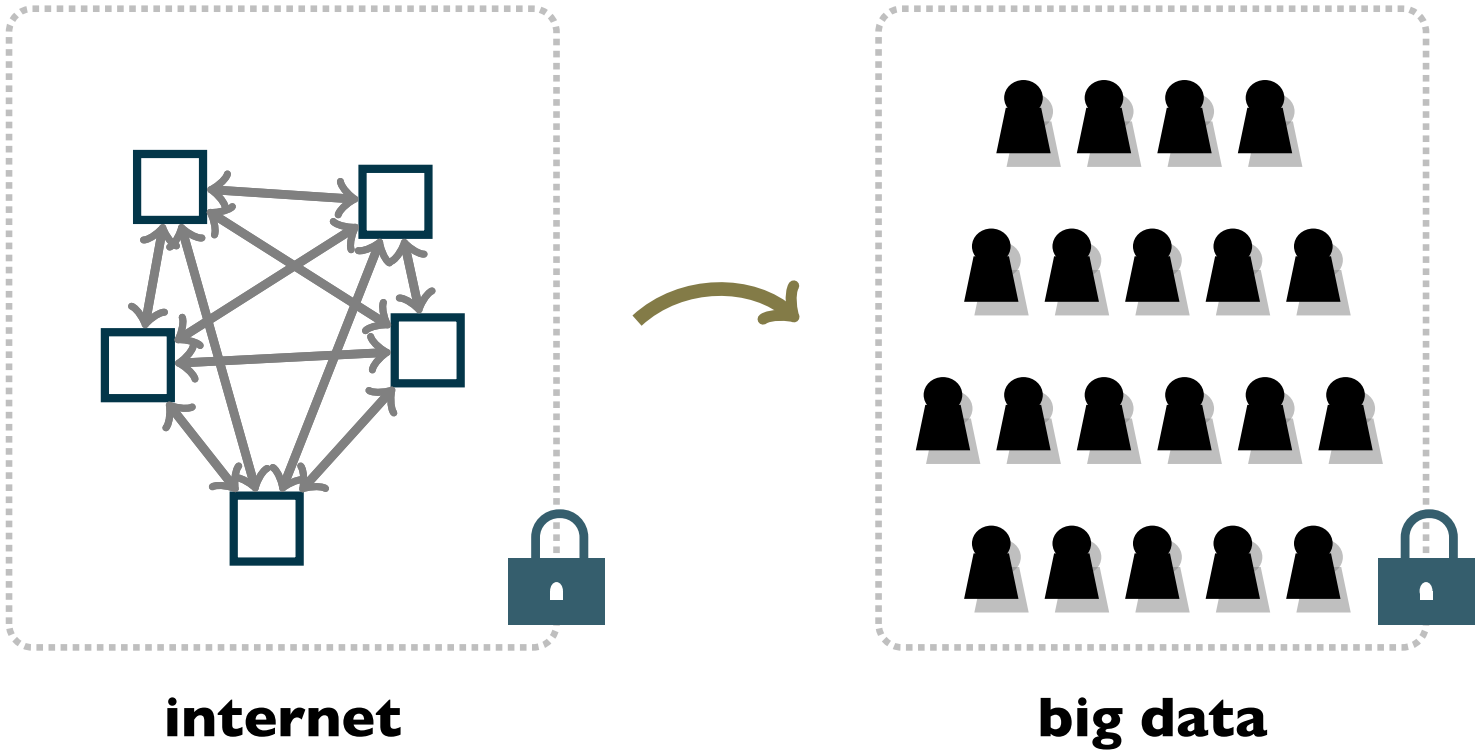
vision. use of **functional encryption**

to secure our data and our computation



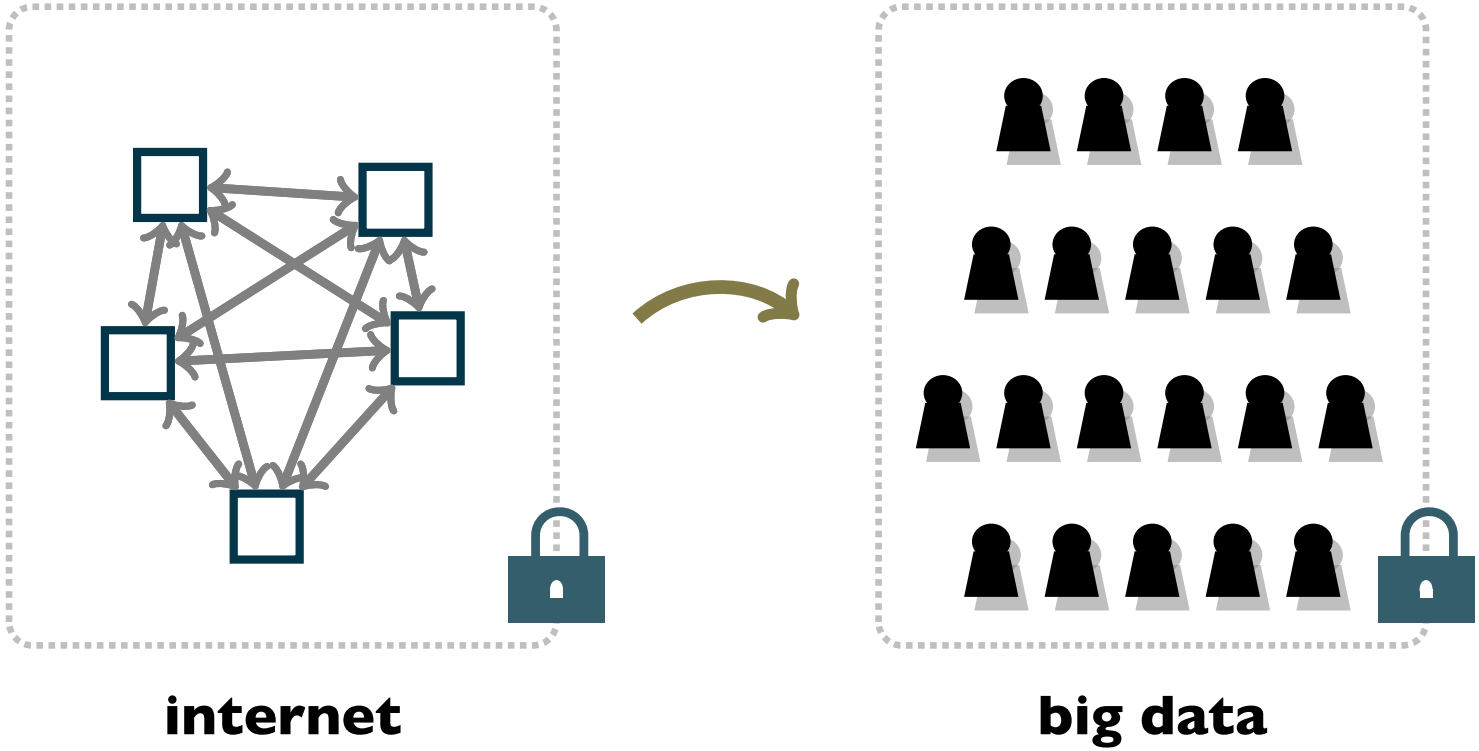
vision. use of **functional encryption**

to secure our data and our computation



vision. use of **functional encryption**

to secure our data and our computation



internet **big data**

pariscryptoday.github.io // **thank you**