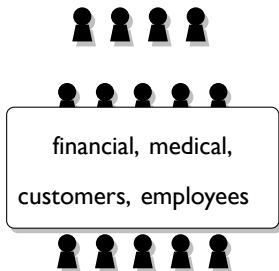


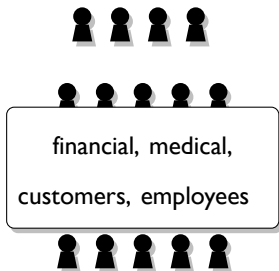
Cryptography, Encryption, *and* Big Data



Hoeteck Wee
ENS, Paris

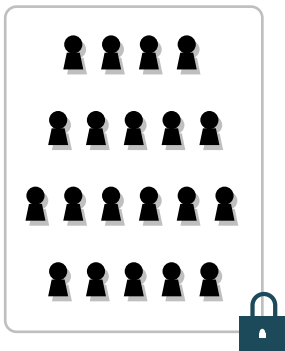


BIG DATA



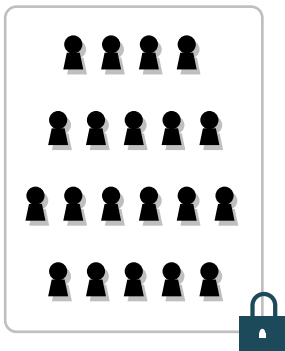
BIG DATA

Q. privacy?



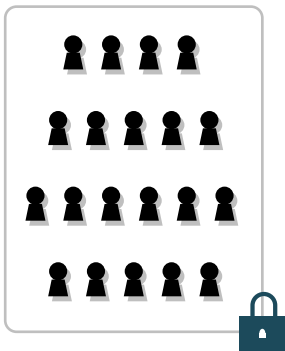
BIG DATA

Q. privacy?



BIG DATA

Q. utility + privacy?



BIG DATA

Q. utility + privacy?

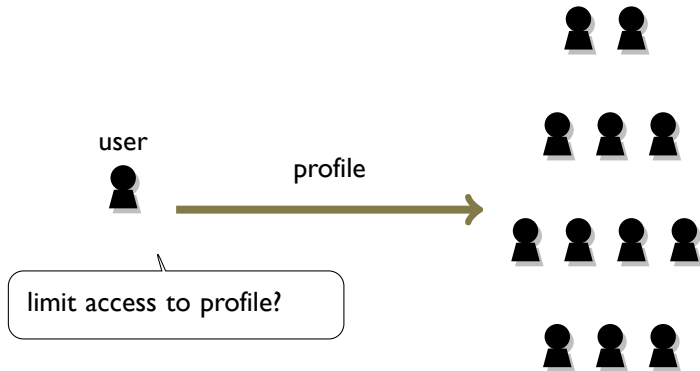
restrict **access** + **computation**

dating + big data

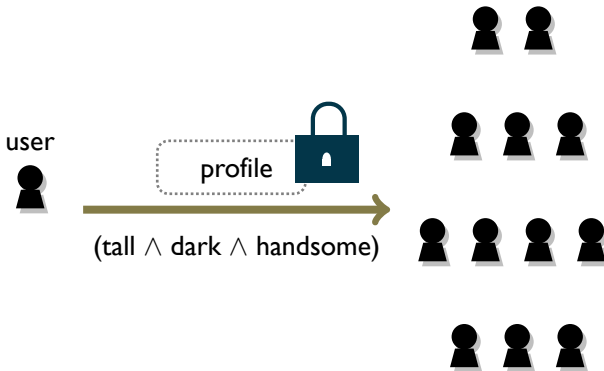
user



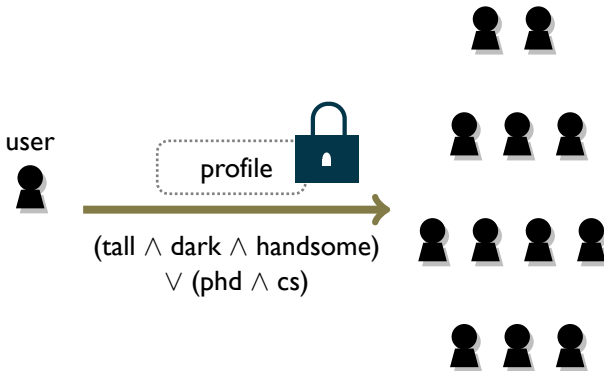
dating + big data



dating + big data



dating + big data



attribute-based encryption



$cs \wedge phd$



cs phd



cs msc



bio phd

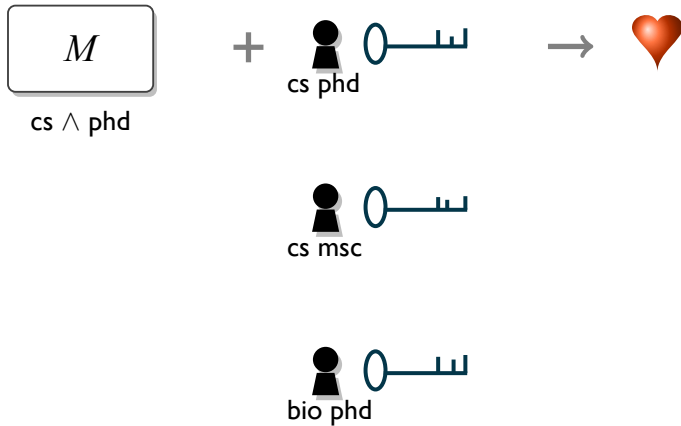
attribute-based encryption



$cs \wedge phd$



attribute-based encryption



attribute-based encryption



$cs \wedge phd$



$cs \text{ } phd$



$cs \text{ } msc$



$bio \text{ } phd$



attribute-based encryption

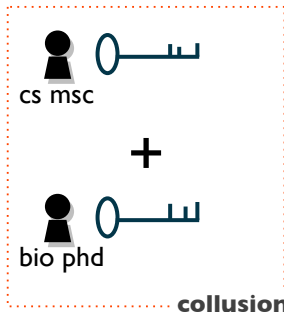


$cs \wedge phd$

+



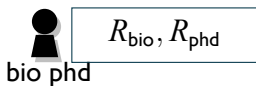
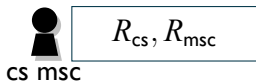
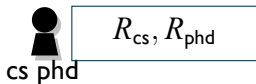
$cs \text{ phd}$




attribute-based encryption




$cs \wedge phd$




attribute-based encryption


$$M \oplus R_{cs} \oplus R_{phd}$$


$cs \wedge phd$


$$R_{cs}, R_{phd}$$

cs phd


$$R_{cs}, R_{msc}$$

cs msc


$$R_{bio}, R_{phd}$$

bio phd

attribute-based encryption

$$\underbrace{M \oplus R_{cs} \oplus R_{phd}}_{cs \wedge phd} + \underbrace{\text{cs phd}}_{\text{cs phd}} \rightarrow M$$

$$\underbrace{\text{cs msc}}_{\text{cs msc}} \rightarrow R_{cs}, R_{msc}$$

$$\underbrace{\text{bio phd}}_{\text{bio phd}} \rightarrow R_{bio}, R_{phd}$$

attribute-based encryption

$$M \oplus R_{cs} \oplus R_{phd}$$

$cs \wedge phd$



cs phd

$$R_{cs}, R_{phd}$$

+



cs msc

$$R_{cs}, R_{msc}$$



+

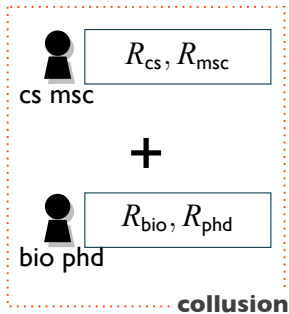
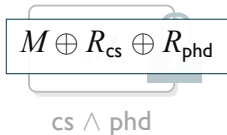


bio phd

$$R_{bio}, R_{phd}$$



attribute-based encryption



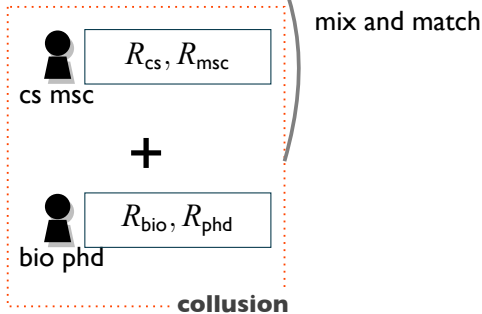
attribute-based encryption

$$M \oplus R_{cs} \oplus R_{phd}$$

$cs \wedge phd$

cs phd

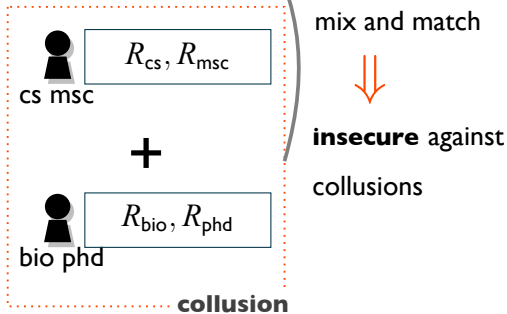
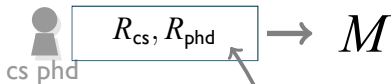
$$R_{cs}, R_{phd} \rightarrow M$$



attribute-based encryption

$$M \oplus R_{cs} \oplus R_{phd}$$

$cs \wedge phd$



attribute-based encryption

[GVW13] **ABE for circuits**

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

one-use \rightarrow many-use

R_{cs}, R_{phd}

R_{cs}, R_{msc}

cs msc

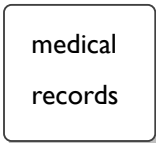
mix and match



bio phd

R_{bio}, R_{phd}

functional encryption [SW05, GPSW06, BSW11]



doctor



receptionist



insurance

functional encryption [SW05, GPSW06, BSW11]



doctor



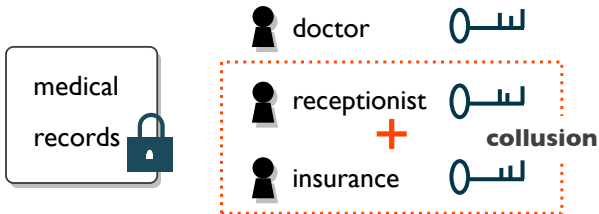
receptionist



insurance



functional encryption [SW05, GPSW06, BSW11]



functional encryption [SW05, GPSW06, BSW11]



doctor



receptionist







insurance





functional encryption [SW05, GPSW06, BSW11]





 $f_1 \rightarrow f_1(D)$ 



 $f_2 \rightarrow f_2(D)$ 



 $f_3 \rightarrow f_3(D)$ 

functional encryption [SW05, GPSW06, BSW11]



 $f_1 \rightarrow f_1(D)$ 

 $f_2 \rightarrow f_2(D)$ 

 $f_3 \rightarrow f_3(D)$ 



fully homomorphic encryption (FHE)



- encrypted answers
- unrestricted computation





functional encryption [SW05, GPSW06, BSW11]



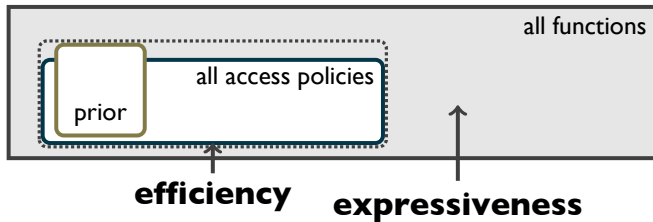
 $f_1 \rightarrow f_1(D)$ 

 $f_2 \rightarrow f_2(D)$ 

 $f_3 \rightarrow f_3(D)$ 

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

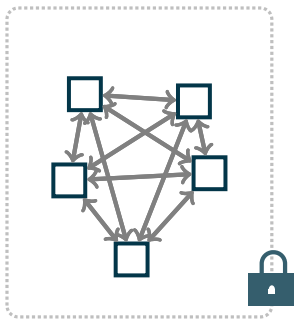
my research



goal. advances in foundations of functional encryption

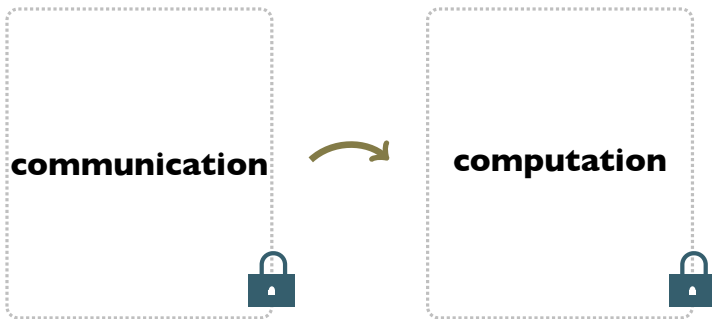
communication



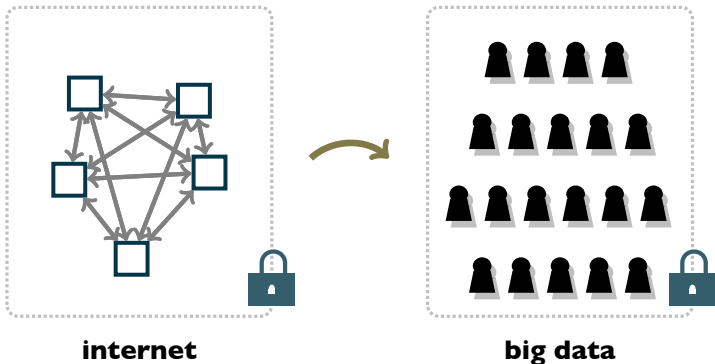


internet

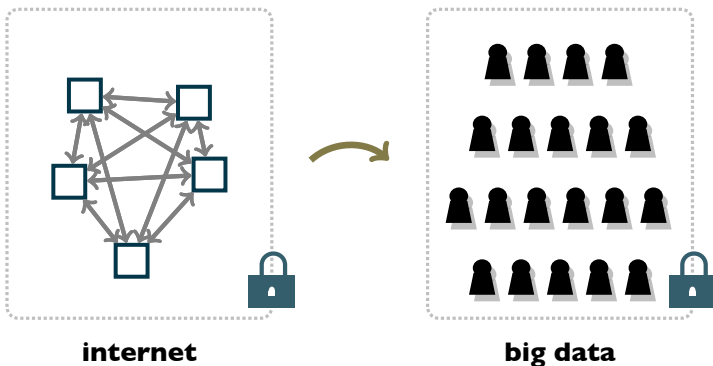
vision. use of **functional encryption**
to secure our data and our computation



vision. use of **functional encryption**
to secure our data and our computation



vision. use of **functional encryption**
to secure our data and our computation



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