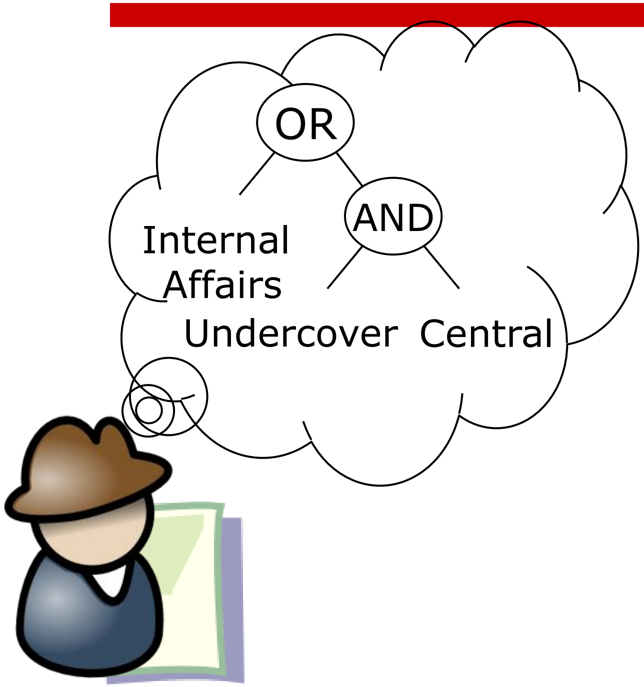
Adaptive Security in Attribute-Based Encryption

Allison Lewko Amit Sahai Brent Waters

Rethinking Encryption

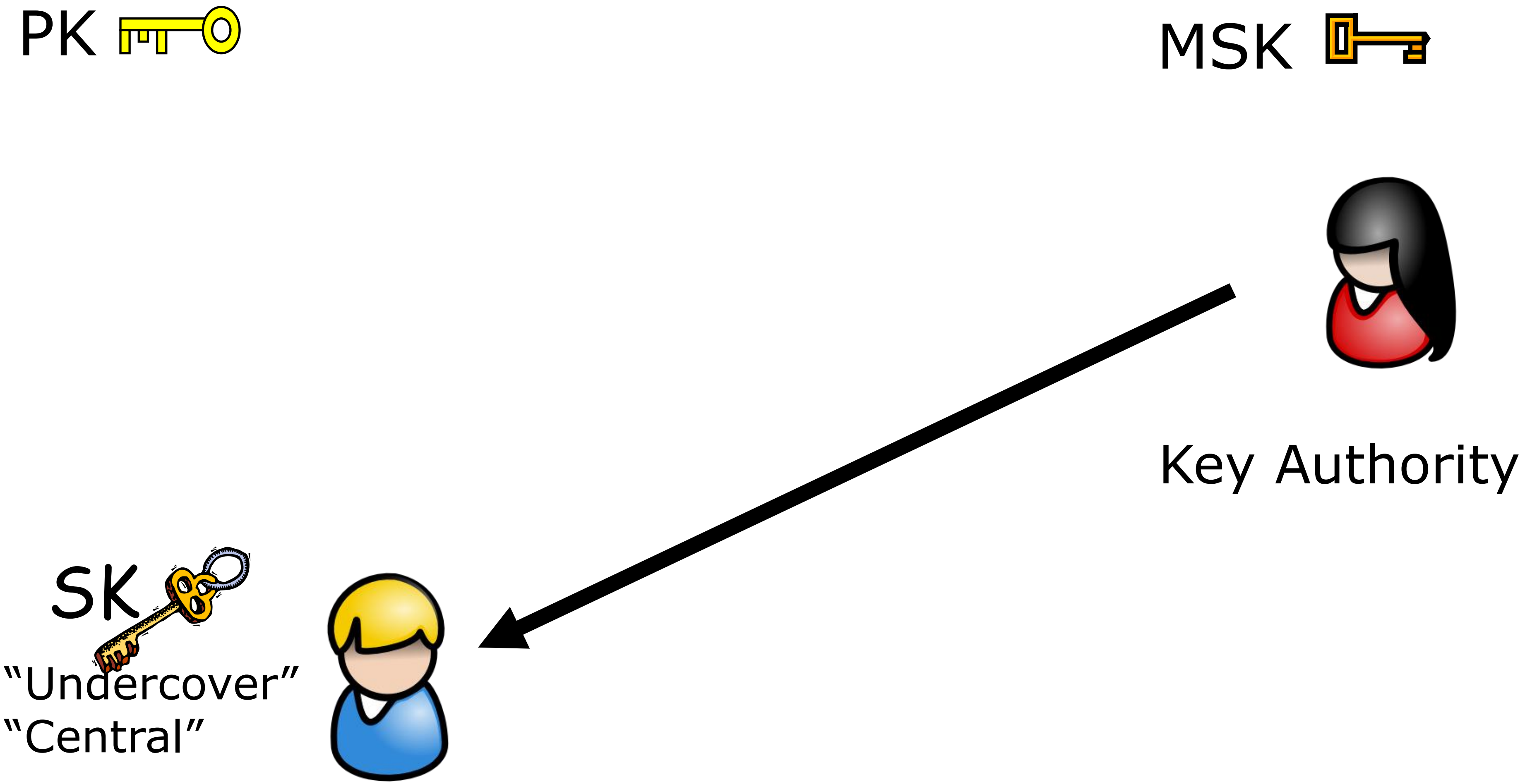


Problem: Disconnect between policy and mechanism

?

- ❑ Who matches this? Am I allowed to know?
- ❑ What if they join later?
- ❑ Should they see everything?
- ❑ Process data before decryption?

Attribute-Based Encryption [SW05]



PK

MSK

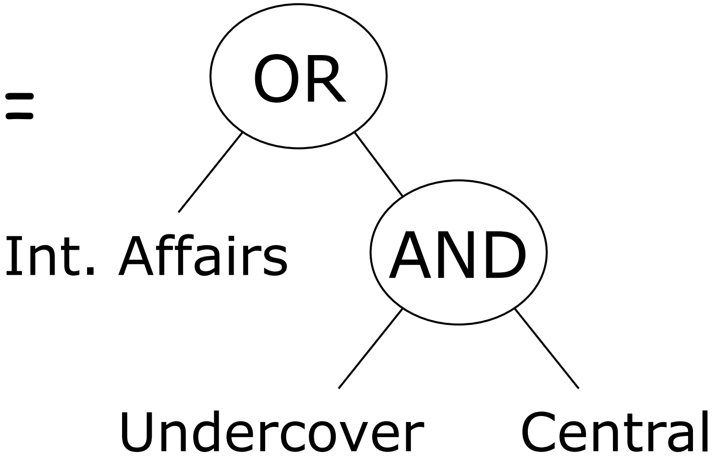
Key Authority

SK

"Undercover"
"Central"

Attribute-Based Encryption [SW05]

ϕ =



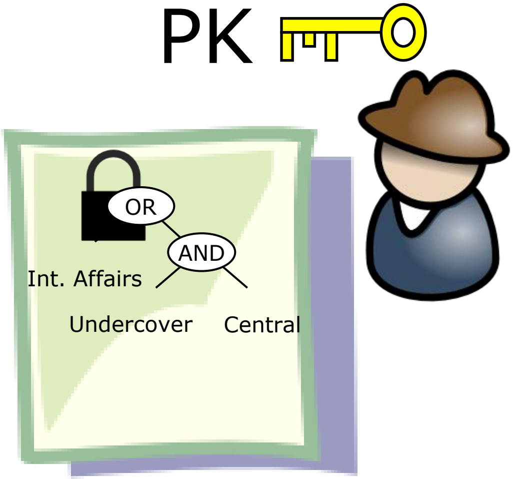
OR

Int. Affairs

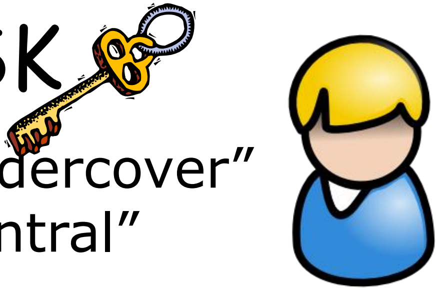
AND

Undercover

Central



PK



SK

“Undercover”
“Central”

Results

Prior: Selective Security

- Declare challenge CT before seeing PK

New: Full/Adaptive Security

- Dual System Encryption W09
- + New Techniques

Thank you