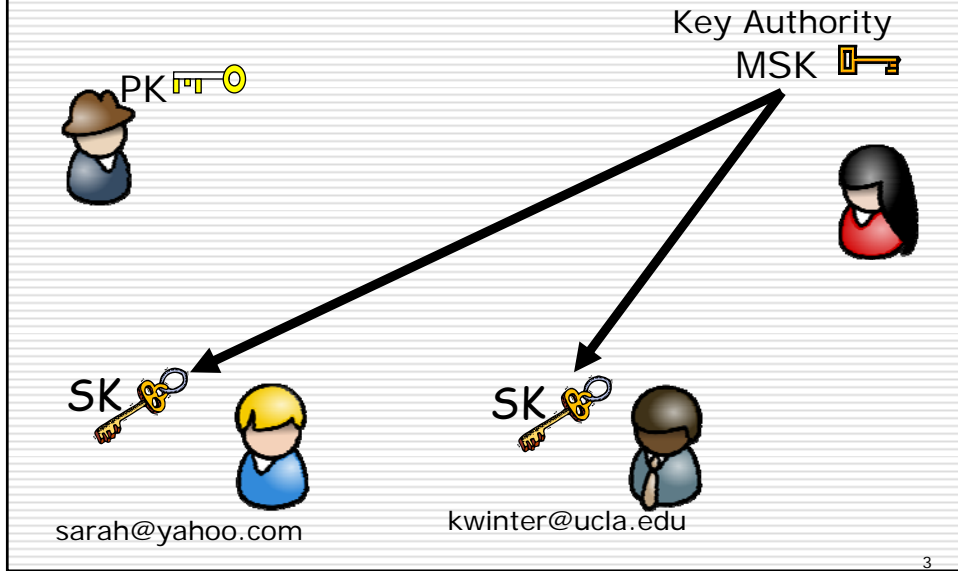


Identity-Based Encryption: A Long Term Perspective

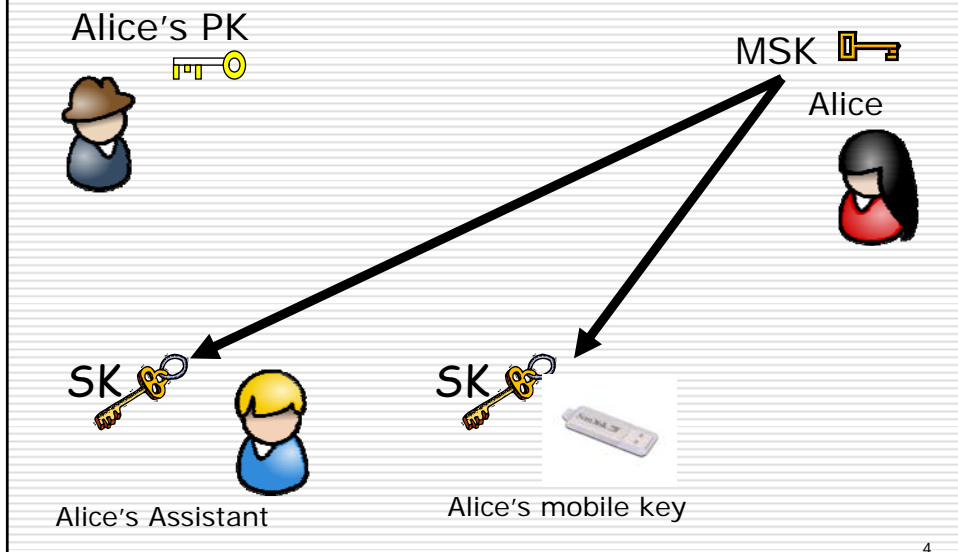
Brent Waters
SRI International

What is IBE?

Traditional View



Managing Your Own Data



Application versus a Technology

- Mistake not to separate
- Think bigger!
- Need to undo bias

5

Three Reasons to Like IBE

Several Applications

- Key Insulation/Forward Security [CHK03...]
- Searching on Encrypted Data [BDOP04]
- Malware Resistance [CDDLLW07]
- Note: none of these have trusted auth.

7

Big Conceptual Idea

- The breakthrough in encryption
- Open for 17 years
- I like big ideas!

8

Thinking Back to Public Key Crypto

- Before: Do we really need it?
- Engineer around it?
- Now:
 - SSL
 - Software Patches

9

Thank you

10