On the Risks of IBE*

Himanshu Khurana and Jim Basney
NCSA, University of Illinois

Midwest Security Workshop, UIUC, Sep 30 2006

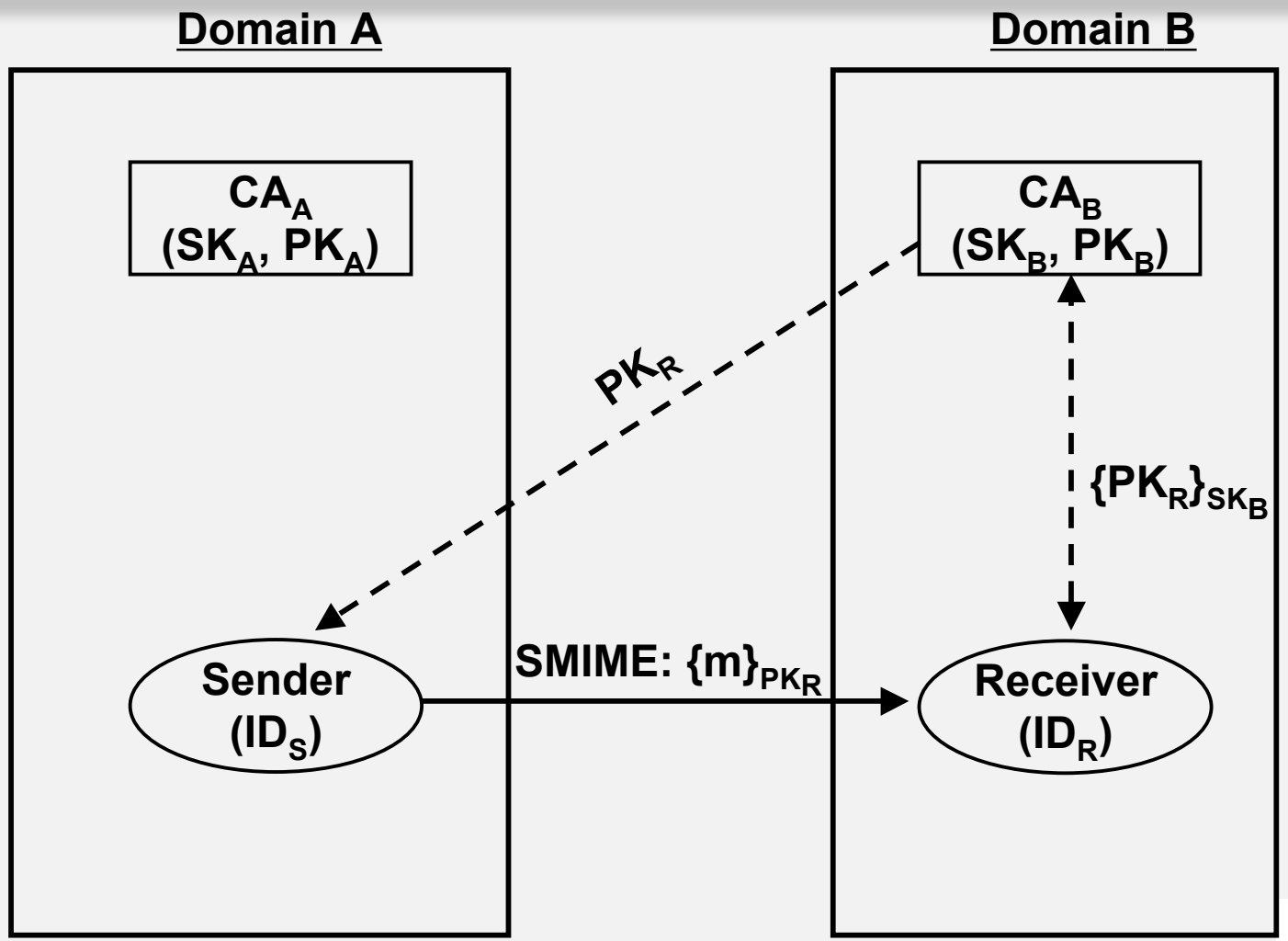
* Accepted at the International Workshop on Applied PKC (IWAP), Dalian, China, Nov 2006

Introduction

- **Identity based cryptography flourishing**
  - Initial work by Cocks, Boneh and Franklin
- **Encrypted email is a killer app for IBE** (Identity Based Encryption)
  - Primary benefit: eliminate key distribution
- **We analyze IBE for Email and argue that**:
  - IBE brings significant *risks* to email security
    - Stronger trust assumptions
    - Unnecessarily complex cryptosystem
      - Can easily be replaced by other cryptosystems; e.g., RSA

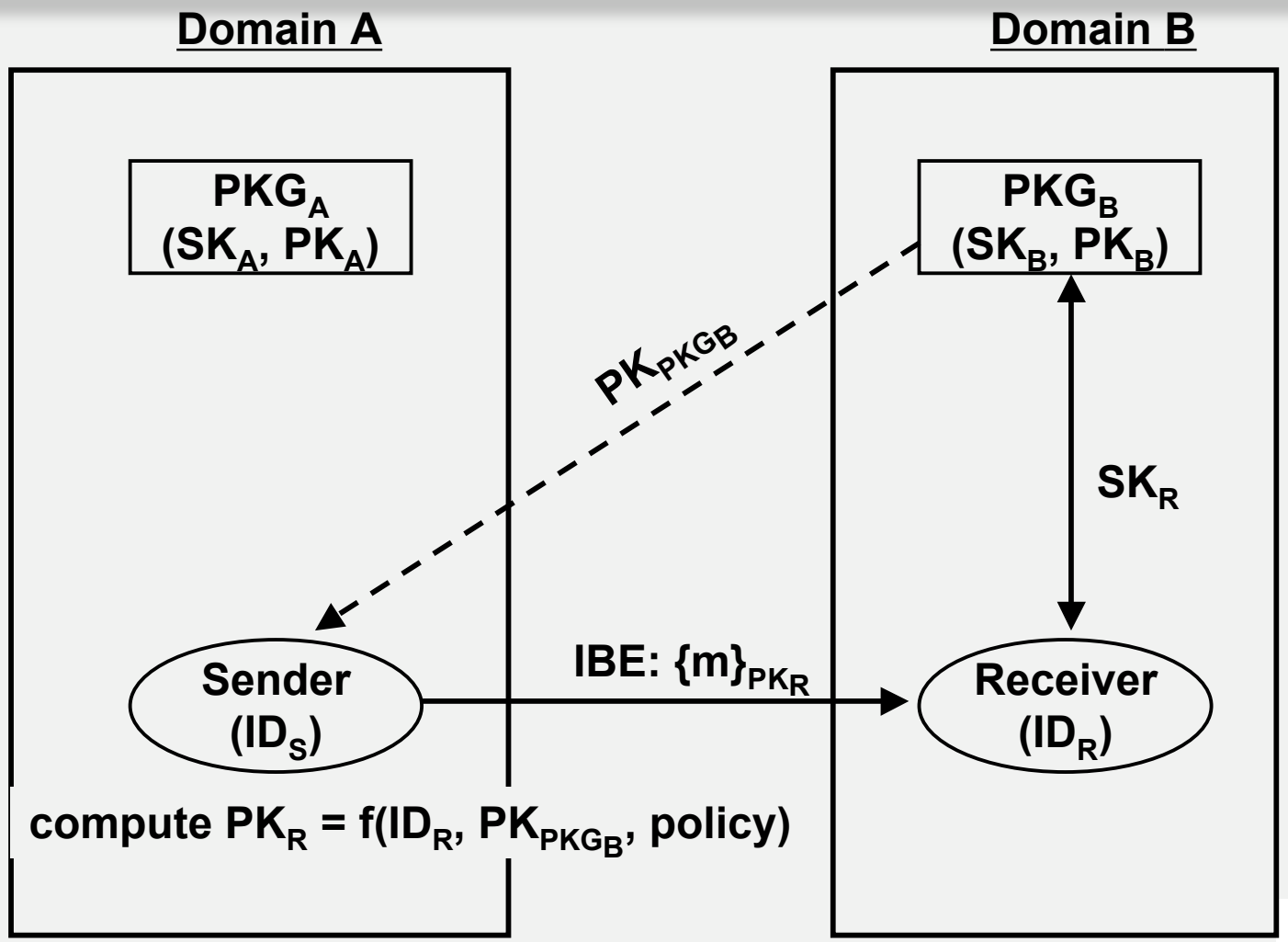
NCSA

Secure Email with RSA (SMIME)



NCSA

Secure Email with IBE



Benefits of IBE

- **Eliminate User Key Distribution**
  - One key fetch per domain (PKG)
  - Sender generates public keys of domain users
- **Policy-based encryption**
  - E.g., “open after Monday”
- **Implicit user mobility**
  - Recipient can get private key from any location on to any device

NCSA

Trust Assumptions
IBE vs. RSA

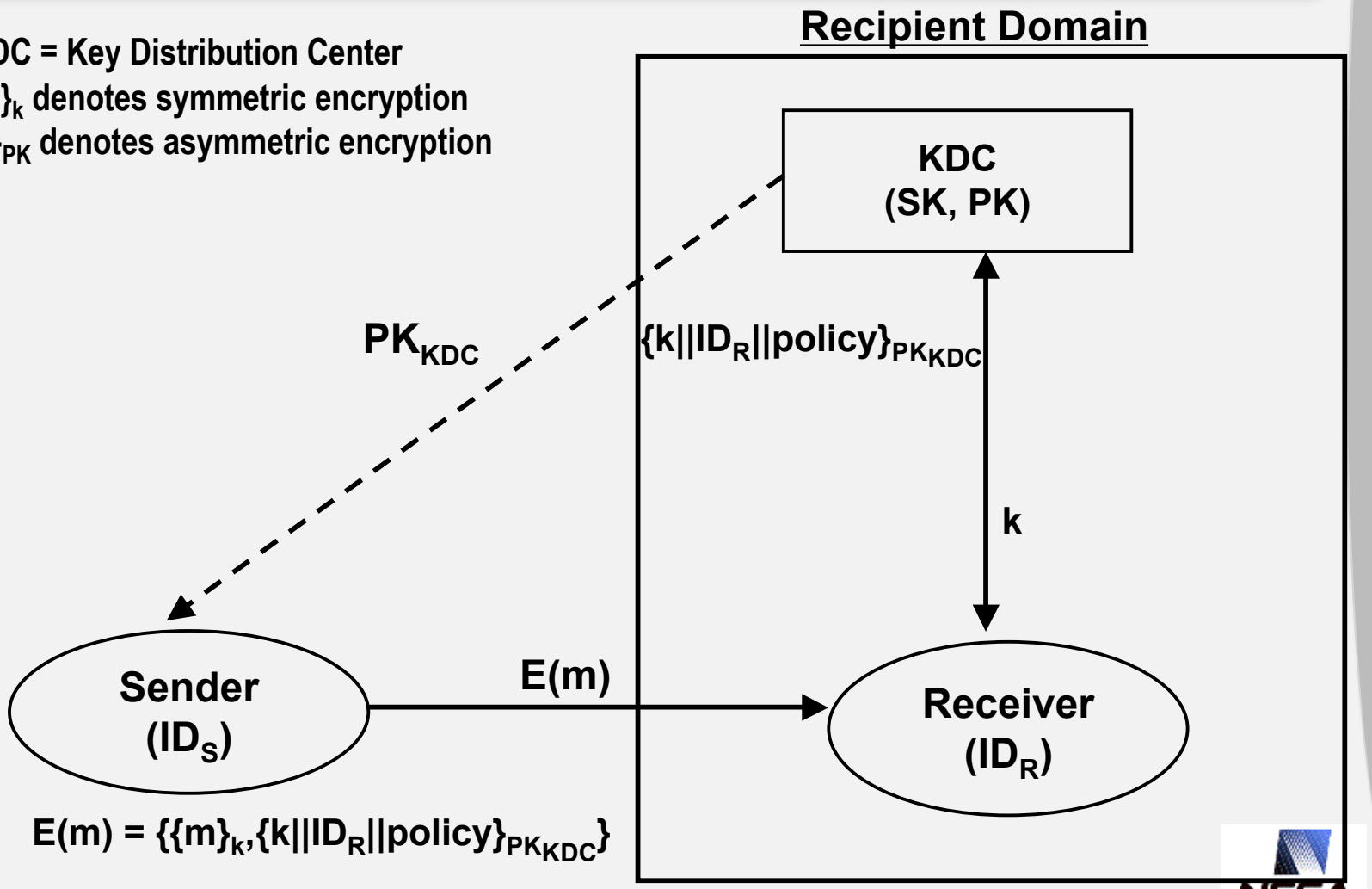
- **Fully trusted PKG**
  - Generates private keys
- **Online PKG**
  - Revocation via short-lived keys
- **Weaker end-to-end encryption**
  - PKG can decrypt messages

- **Partially trusted CA**
  - Users generate keys
- **Offline CA**
  - Revocation via CRLs, OCSP
- **Strong end-to-end encryption**
  - Only recipient can decrypt messages

NCSA

Secure Email with IB-MKD
(Identity Based - Message Key Distribution)

- KDC = Key Distribution Center
- $\{m\}_k$ denotes symmetric encryption
- $\{x\}_{PK}$ denotes asymmetric encryption



Analysis

- **IB-MKD achieves IBE benefits, same trust assumptions**
  - Using widely-accepted RSA cryptosystem
  - Previous work fails to do so [Ding03, Callas05]

- **Protocol differences in IB-MKD**
  - User encrypts with domain public key
    - Highlights weaker notion of end-to-end encryption
    - Does not change security properties
  - Policy itself is encrypted
    - Additional feature not provided in IBE
  - Recipient must contact KDC for every message
    - More overhead than IBE but comparable to SSL POP; i.e., reasonable
    - Provides timely policy evaluation

NCSA

Conclusions

- **Secure Email with IBE has strong trust assumptions**
  - Need to be evaluated carefully before deployment
- **IBE's complex cryptography may be unnecessary**
  - IB-MKD achieves goals with RSA
- **Questions**?
  - hkhurana@ncsa.uiuc.edu

NCSA