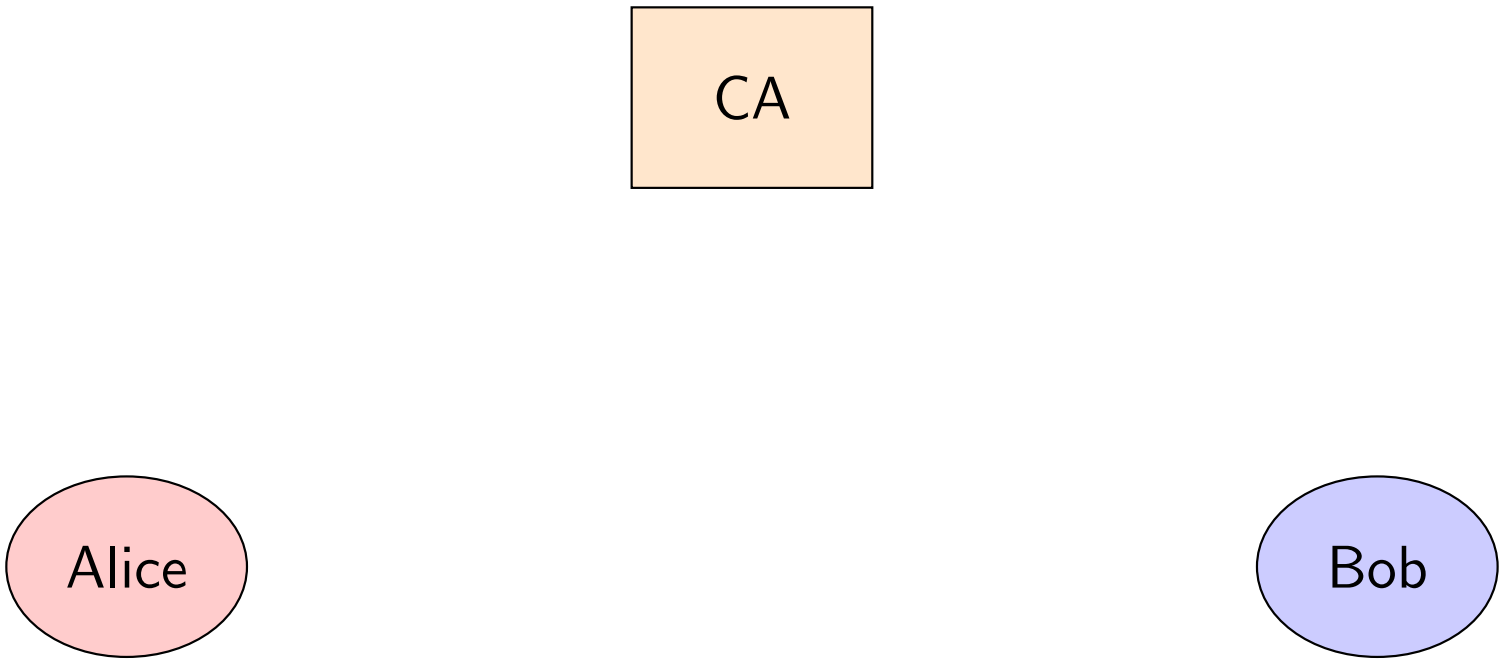
Spatial Encryption

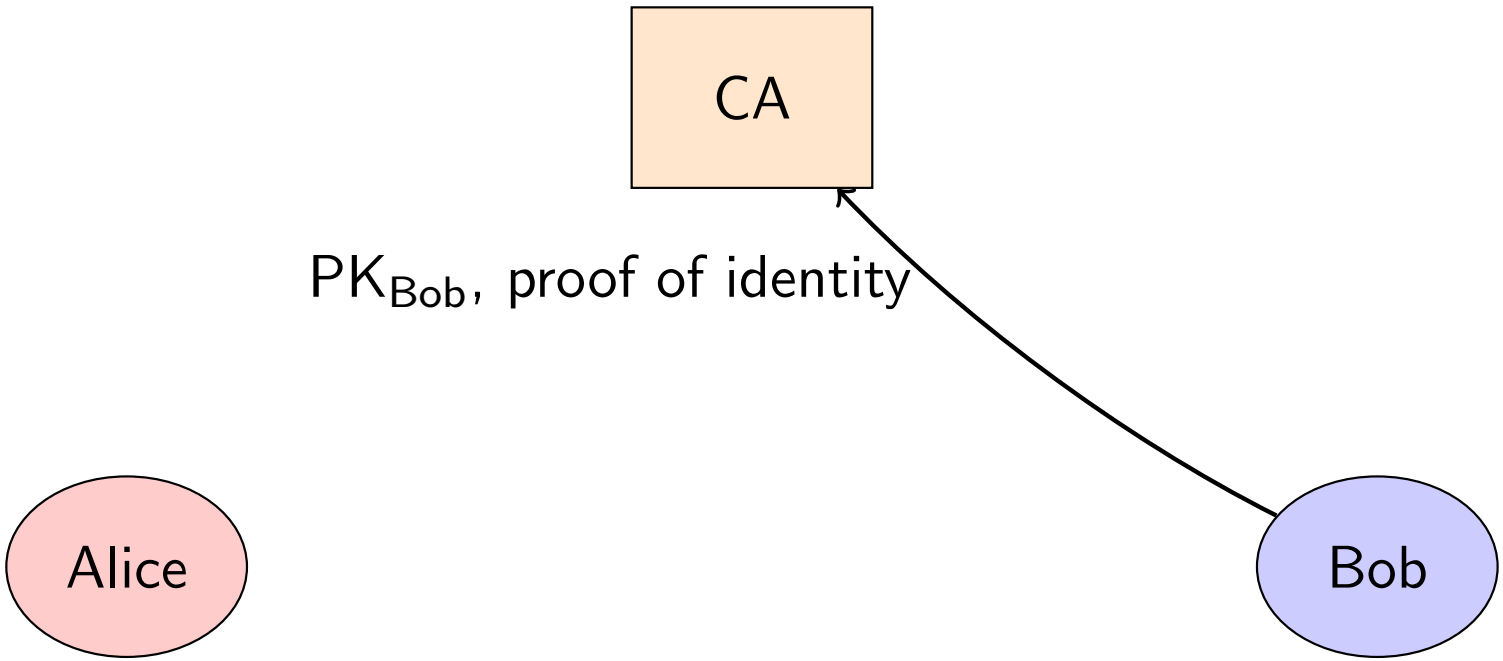
Adam Barth Dan Boneh Mike Hamburg

March 17, 2008

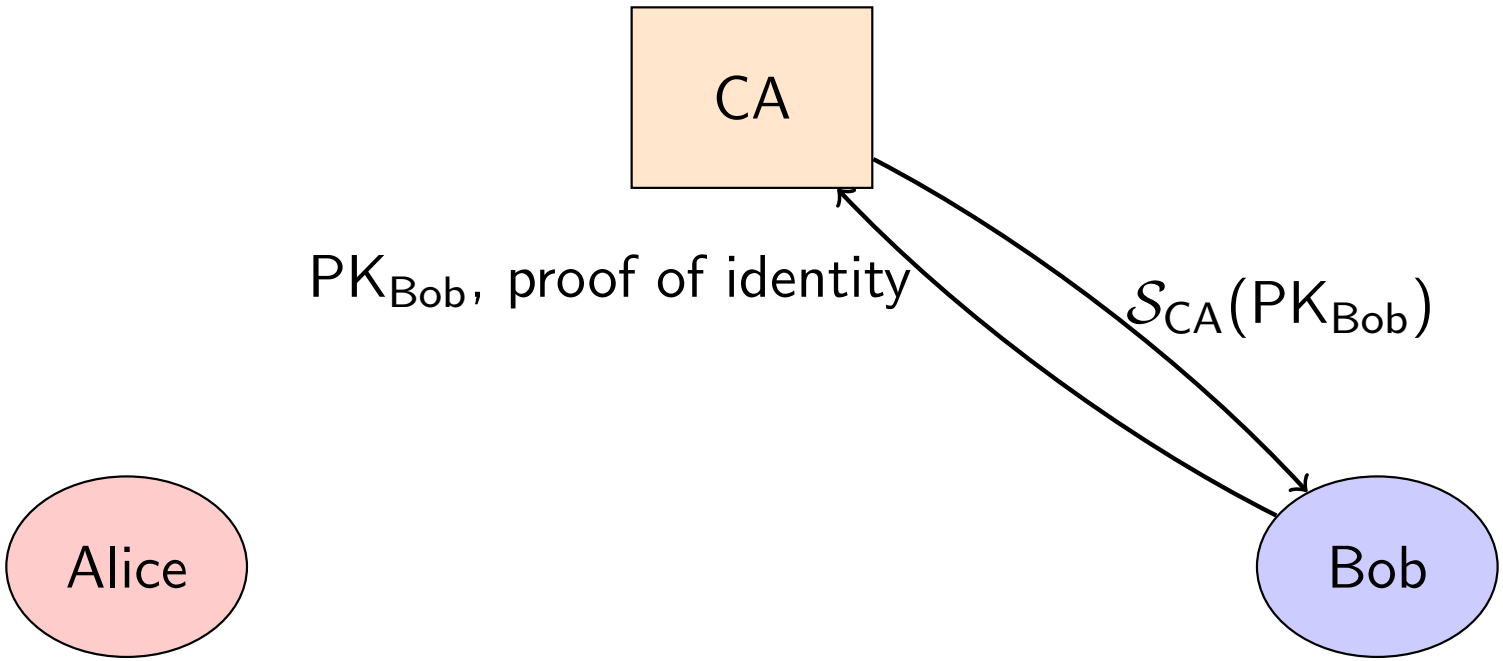
Traditional Public-Key Infrastructure



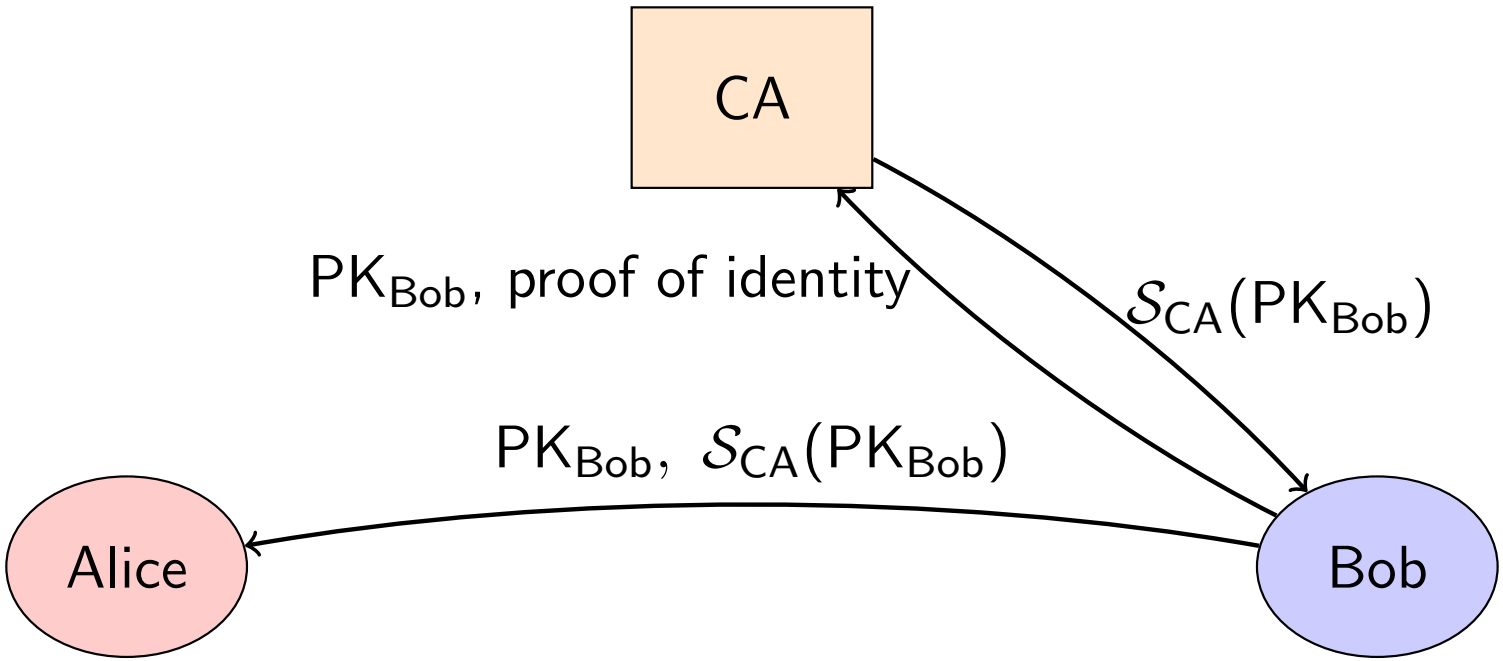
Traditional Public-Key Infrastructure



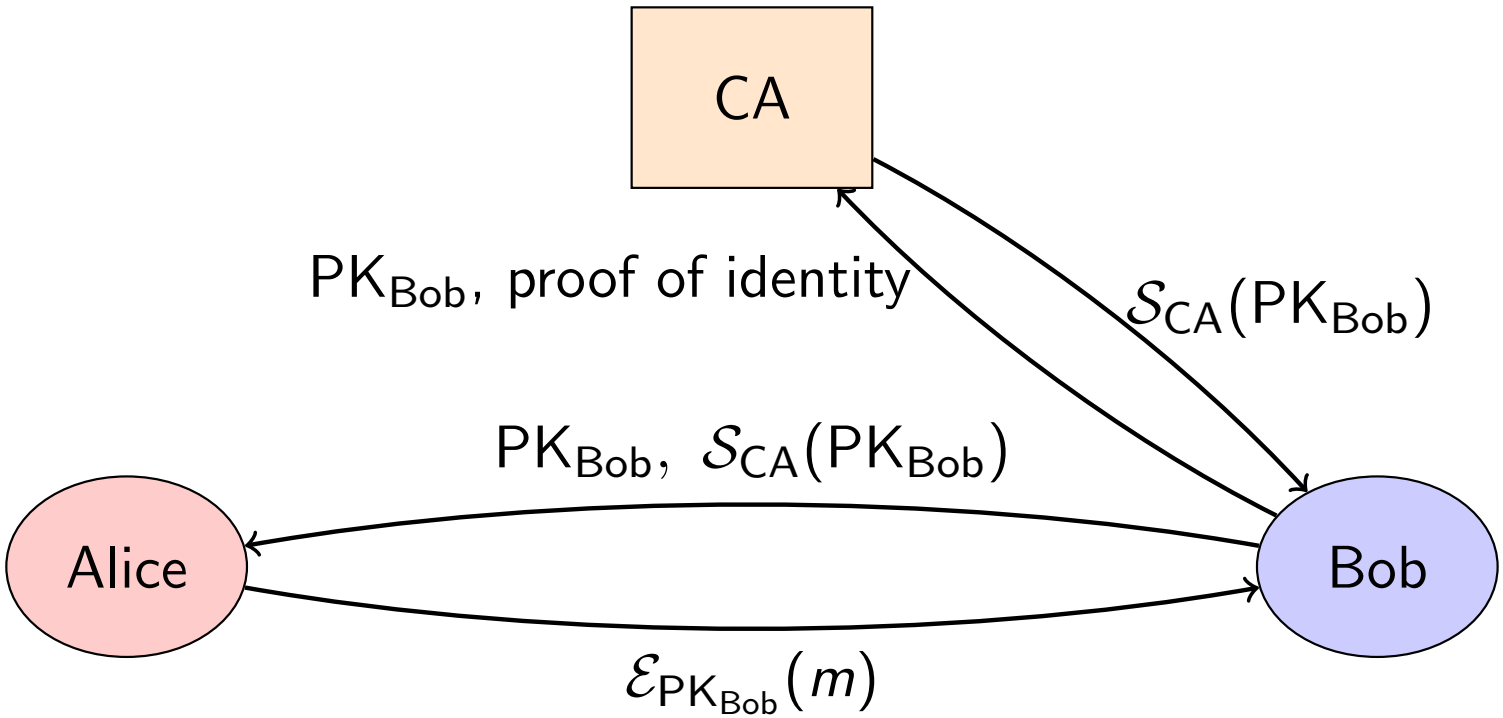
Traditional Public-Key Infrastructure



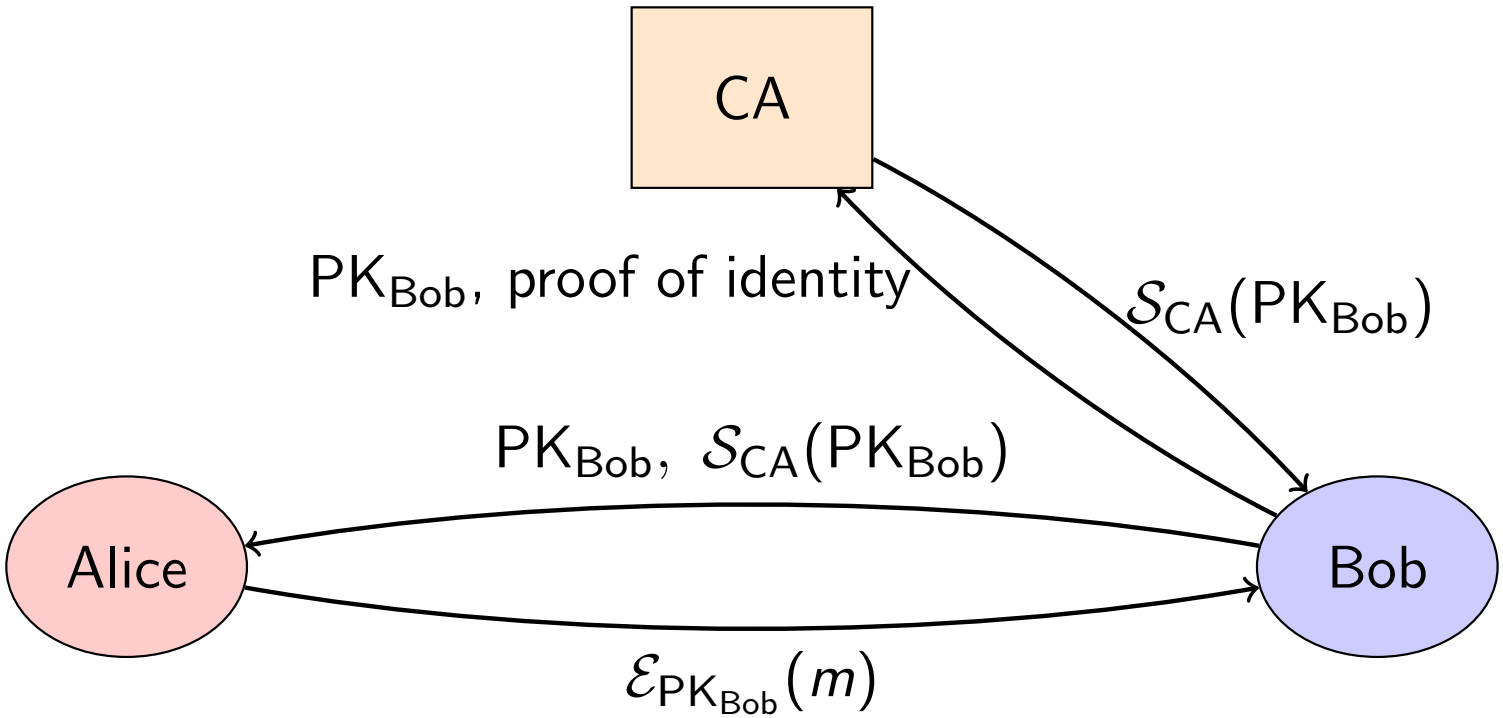
Traditional Public-Key Infrastructure



Traditional Public-Key Infrastructure



Traditional Public-Key Infrastructure



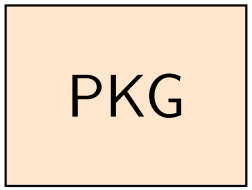
But for email, Bob is offline!

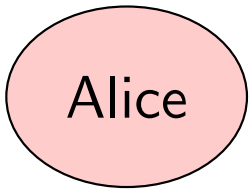
Identity-Based Encryption

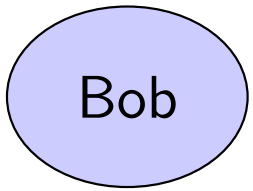
- Public key can be any string
- Private key given by trusted authority

Identity-Based Encryption

- Public key can be any string
- Private key given by trusted authority

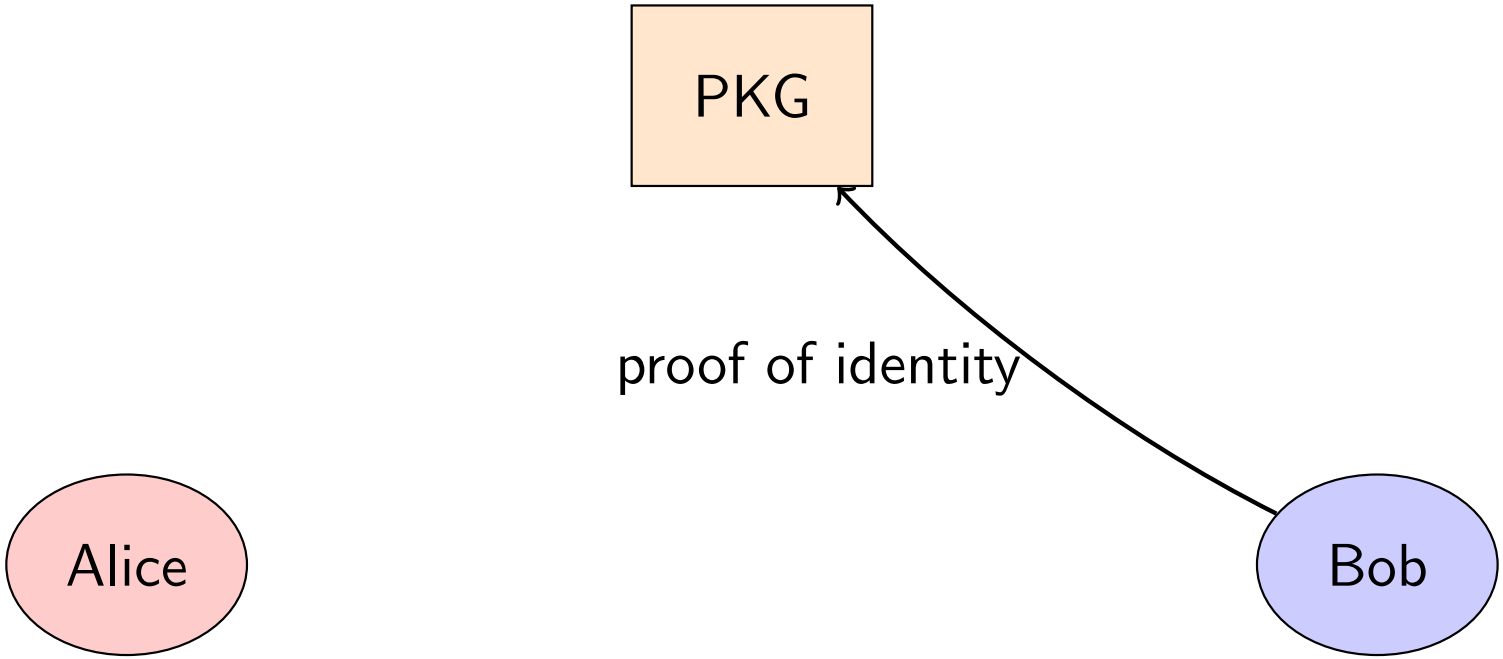






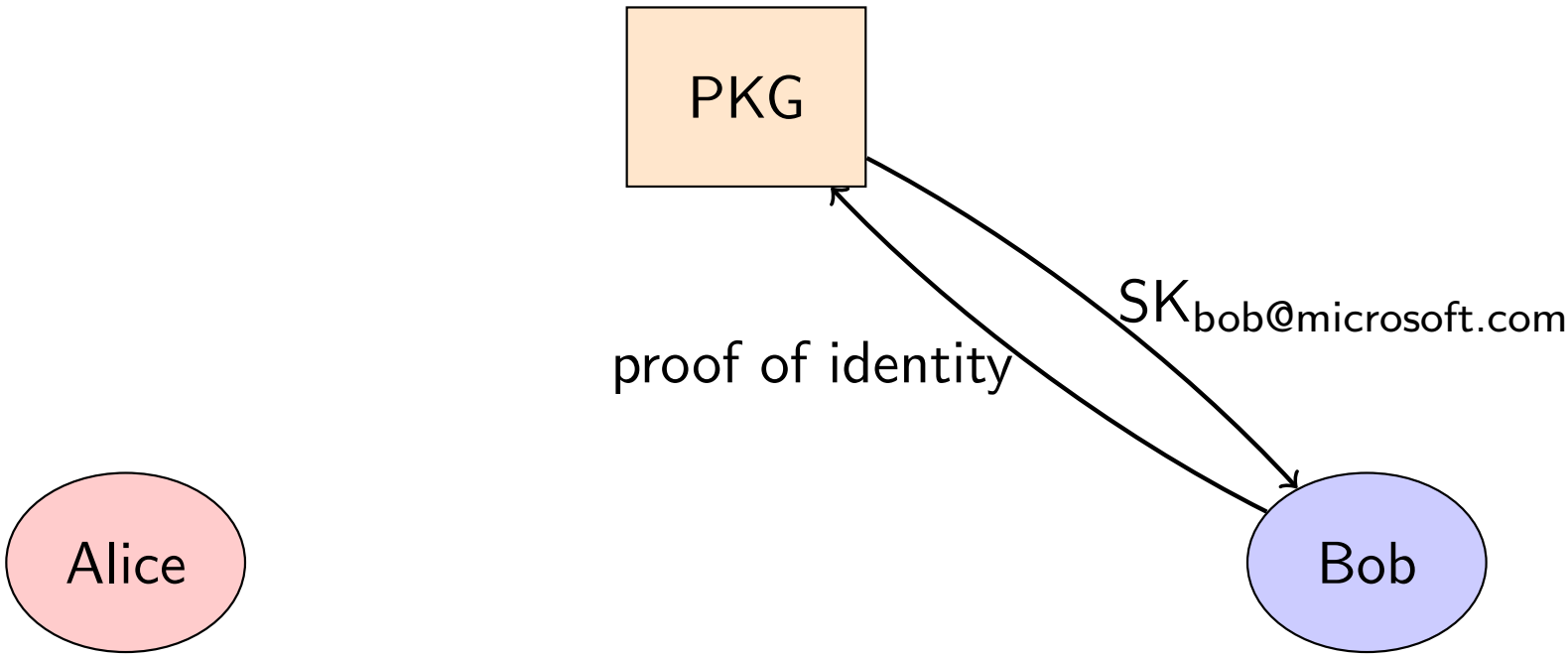
Identity-Based Encryption

- Public key can be any string
- Private key given by trusted authority



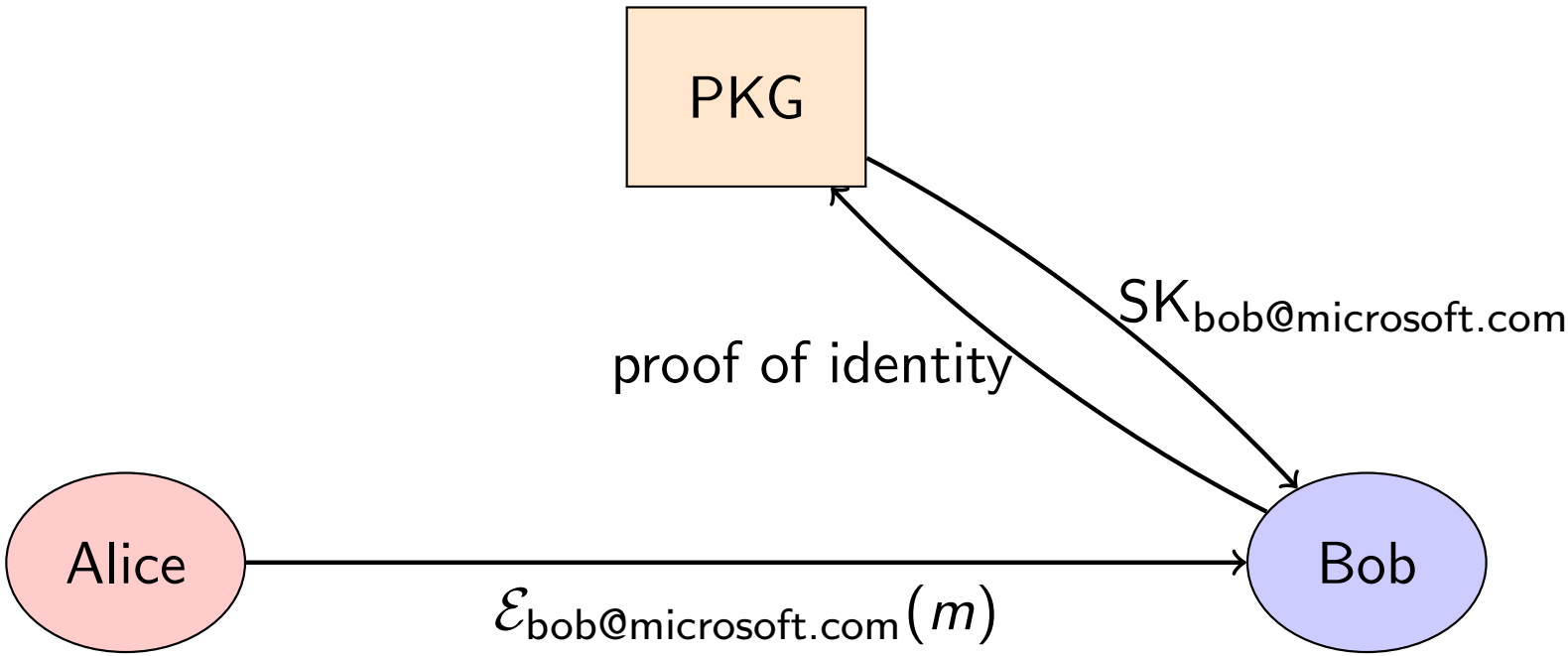
Identity-Based Encryption

- Public key can be any string
- Private key given by trusted authority



Identity-Based Encryption

- Public key can be any string
- Private key given by trusted authority



Problems using IBE for Email

- Sending to multiple recipients
  - Lots of ciphertext
  - Solved by broadcast IBE

Problems using IBE for Email

- Sending to multiple recipients
  - Lots of ciphertext
  - Solved by broadcast IBE
- Multiple trusted authorities

Email Encryption Wishlist

- Send to multiple recipients
- Trust in multiple authorities
- Short ciphertexts
- Short public keys
- Short private keys
- No central authority
- Hierarchical delegation

Email Encryption Wishlist

- Send to multiple recipients ✔
- Trust in multiple authorities ✔
- Short ciphertexts ✔ (2 group elements)
- Short public keys ✔ (random oracle model)
- Short private keys ✗ O(max recipient list)
- No central authority ✗
- Hierarchical delegation ✔

Spatial Encryption

- A new primitive
- Identities are points in a vector space
- Keys for any hyperplane
  - Can decrypt at any point in the hyperplane
- Delegate from plane to line to point

Our implementation

- Encryption, decryption are efficient
- Ciphertext is short
- Master public key is long but random
  - Proportional to dimension of vs
  - Short in the random oracle model
- Private keys are long
  - Proportional to dimension of vs

Spatial Encryption for Email

- Vector space is polynomials
- $\mathrm{SK}_{\mathrm{Auth}}$: polys w/root at Auth
- $\mathrm{SK}_{\mathrm{Auth,\ Bob}}$: polys w/roots at Auth, Bob
- Alice encrypts her message to

$$(x - \text{voltage})(x - \text{thawte}) \cdots (x - \text{bob@...}) \cdots (x - \text{zak@...})$$

Hierarchical IBE

- W for $/\text{path}/\text{to}/\text{data}/$ is $(\text{path}, \text{to}, \text{data}, *, \ldots, *)$

Hierarchical IBE

- W for $/\text{path}/\text{to}/\text{data}/$ is $(\text{path}, \text{to}, \text{data}, *, \ldots, *)$

... or ...

- W is $(x - /\text{path})(x - /\text{path}/\text{to})(x - /\text{path}/\text{to}/\text{data}) \cdot Q(x)$
- Enables broadcast HIBE
- Enables delegation for email encryption

Nitty-Gritty

- Based on Boneh-Boyen-Goh H-IBE
- Uses bilinear pairings
- Selective-ID secure in the standard model

Summary

- A new crypto primitive
- Generalization of H-IBE
- Enables efficient email encryption
- Enables broadcast H-IBE

The End

Questions?