Spatial Encryption

Adam Barth    Dan Boneh    Mike Hamburg

March 17, 2008
Traditional Public-Key Infrastructure

- CA
- Alice
- Bob

But for email, Bob is offline!
Traditional Public-Key Infrastructure

PK_{Bob}, proof of identity

Adam Barth, Dan Boneh, Mike Hamburg
Spatial Encryption
Traditional Public-Key Infrastructure

Bob

PK_{Bob}, proof of identity

S_{CA}(PK_{Bob})

CA

Alice

But for email, Bob is offline!

Adam Barth, Dan Boneh, Mike Hamburg

Spatial Encryption
Traditional Public-Key Infrastructure

CA

Bob

PK_{Bob}, proof of identity

S_{CA}(PK_{Bob})

PK_{Bob}, S_{CA}(PK_{Bob})

Alice

But for email, Bob is offline!
Traditional Public-Key Infrastructure

But for email, Bob is offline!

Adam Barth, Dan Boneh, Mike Hamburg  Spatial Encryption
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

PKG

Alice

Bob
Identity-Based Encryption

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

![Diagram showing PKG, Alice, and Bob connected with proof of identity]

Adam Barth, Dan Boneh, Mike Hamburg
Identity-Based Encryption

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

PKG

proof of identity

SK_{bob@microsoft.com}

Alice

Bob

Adam Barth, Dan Boneh, Mike Hamburg

Spatial Encryption
Identity-Based Encryption

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

PKG

Alice

proof of identity

SK_{bob@microsoft.com}

Bob

$E_{bob@microsoft.com}(m)$
Problems using IBE for Email

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

Adam Barth, Dan Boneh, Mike Hamburg
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 ✓
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
- $SK_{Auth}$: polys w/root at Auth
- $SK_{Auth, Bob}$: 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 `/path/to/data/` is `(path, to, data, *, . . . , *)

Enables broadcast HIBE

Enables delegation for email encryption
Hierarchical IBE

- $W$ for /path/to/data/ is (path, to, data, *, ..., *)

... or ...

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