Identity-Based Encryption (IBE)

- The concept (Shamir, 1984): Bob’s public key can be any arbitrary string – e.g., his name or email address (plus the date). The set-up:

  - Private key generator
  - SK
  - ID Bob
  - Proof of Identity
  - E_{ID Bob, PKG}(M)

  - SK_{ID Bob} is a function of ID_{Bob} and PKG’s secret key

  - Alice
  - SK_{ID Bob}
  - Bob
  - PKG’s secret key
  - SK_{ID Bob}
  - M

  - Sent via a secure channel

Hierarchical ID-based Encryption

- What if we have a hierarchy of PKGs rather than a single PKG?
  - Private key generation is local: Bob gets private key from his parent PKG.
  - Improves scalability (offloading computation from root).
  - Makes it easier for Bob to prove identity and get secure channel.
  - Parameters are global: Alice just gets the public key of Bob’s root PKG.
  - Bob’s lower-level PKGs have no public keys.

Security

- Attacker may be able to compromise secret keys of nodes
  - Even choose adaptively the nodes to attack
  - Note: compromising PKG means all its subtree is compromised
  - Still, a node remains secure as long as:
    - Its key was not compromised
    - None of its ancestors was compromised

Our Contribution

- Some prior solutions [GS02,BB04,W05,BBG05,…]
  - But weaker security guarantee
    - Proof of security degrades as O(q^d)
  - So proof is only meaningful for a small constant depth
  - We suggest a new construction and proof
    - Security only degrades linearly with q, independent of d
    - Meaningful also for deep hierarchies