Identity-based Encryption with Efficient Revocation

Alexandra Boldyreva • Vipul Goyal • Virendra Kumar
Georgia Tech UCLA Georgia Tech

(To appear at ACM CCS '08)

Revocation is Important

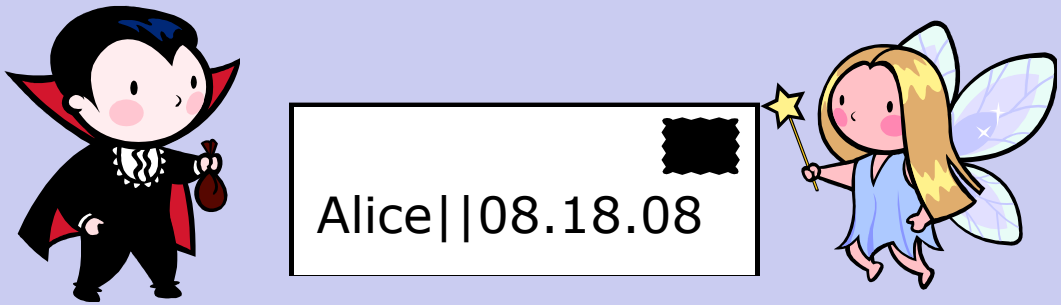
- Key revocation support is important when encryption is used
  - E.g. to limit the use of stolen decryption keys

PKI setting

CRL-online public directory

PK_{Alice}	Valid
PK_{Bob}	Invalid

IBE setting

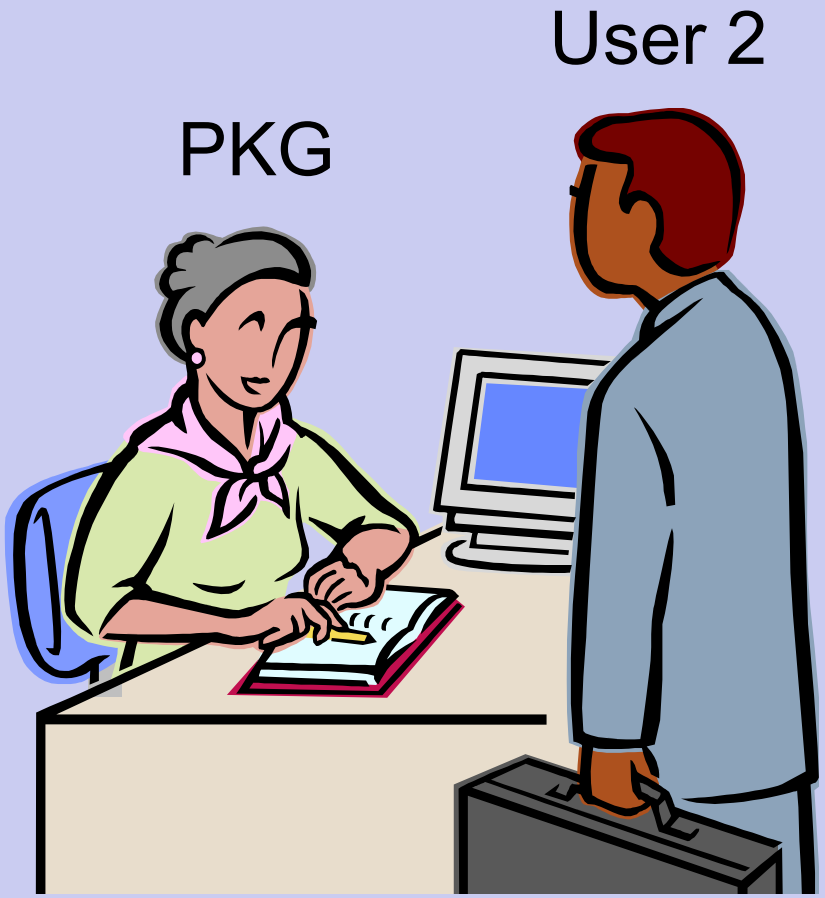


CRL-online public directory

PK_{Alice}	Valid
PK_{Bob}	Inv

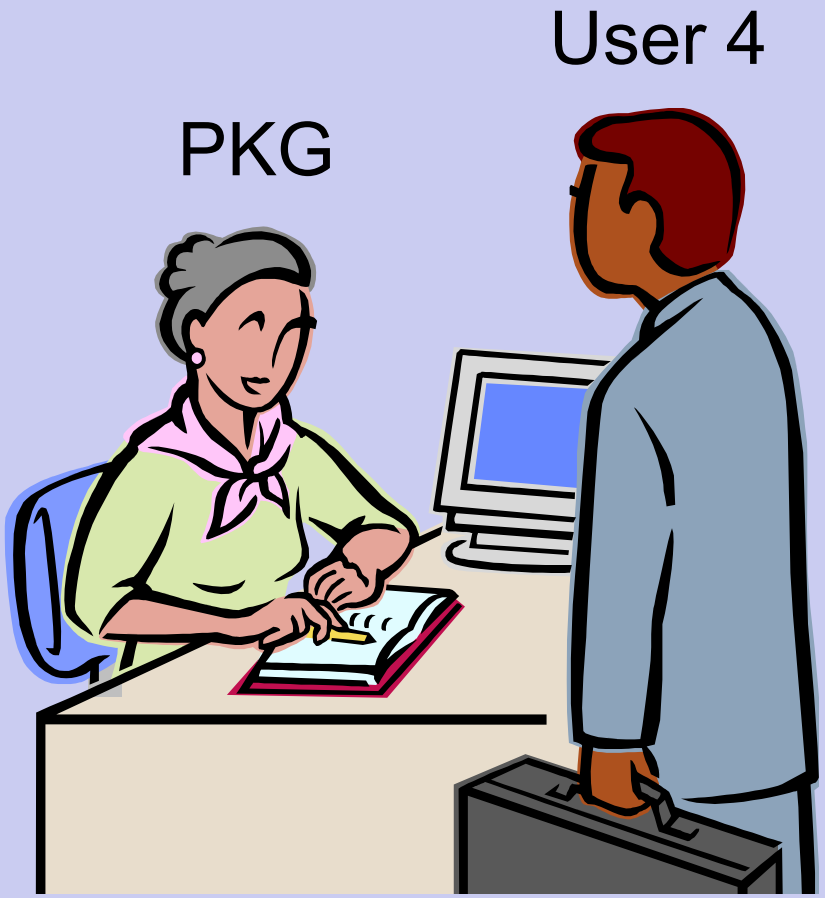
Assume there are 1000 users

Assume there are 1000 users

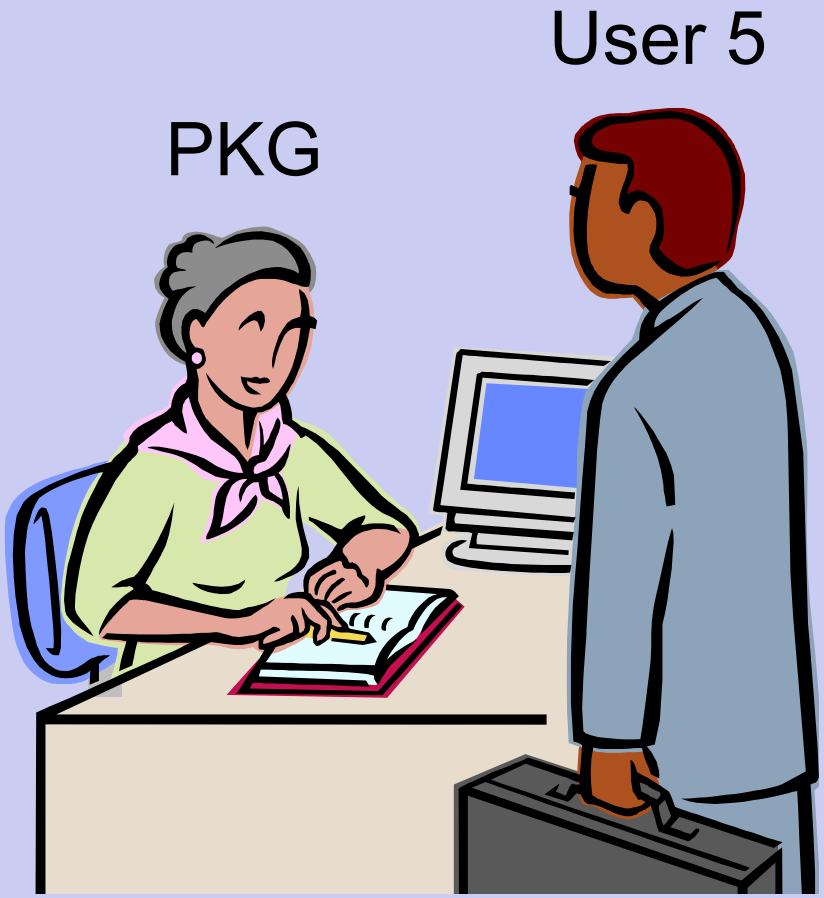


Assume there are 1000 users

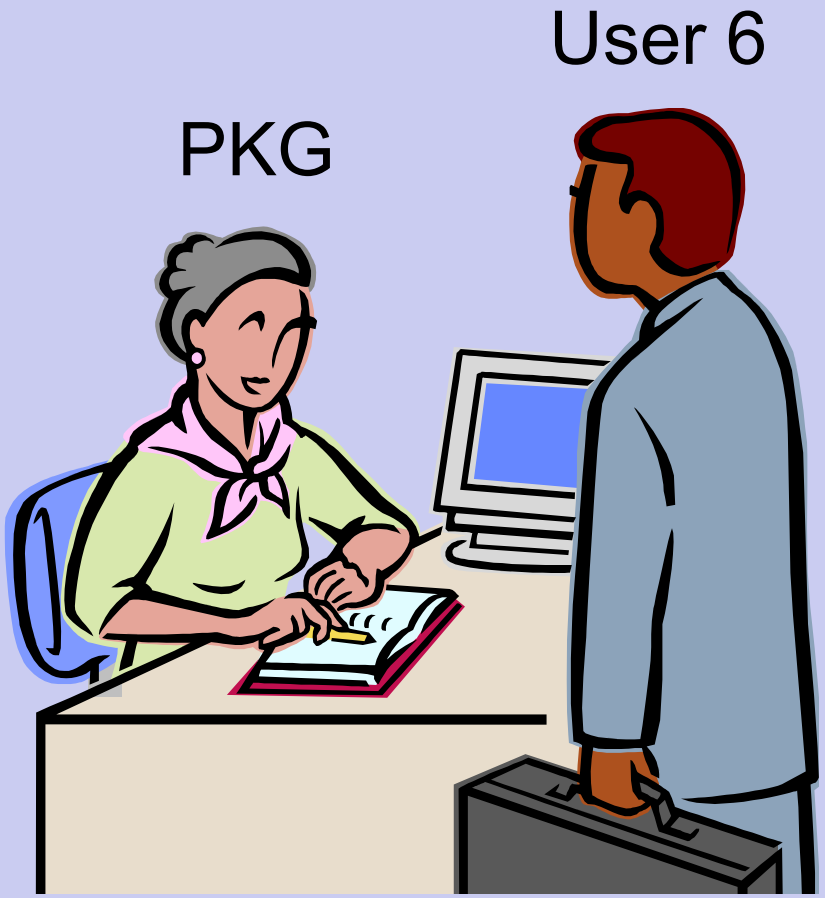
Assume there are 1000 users



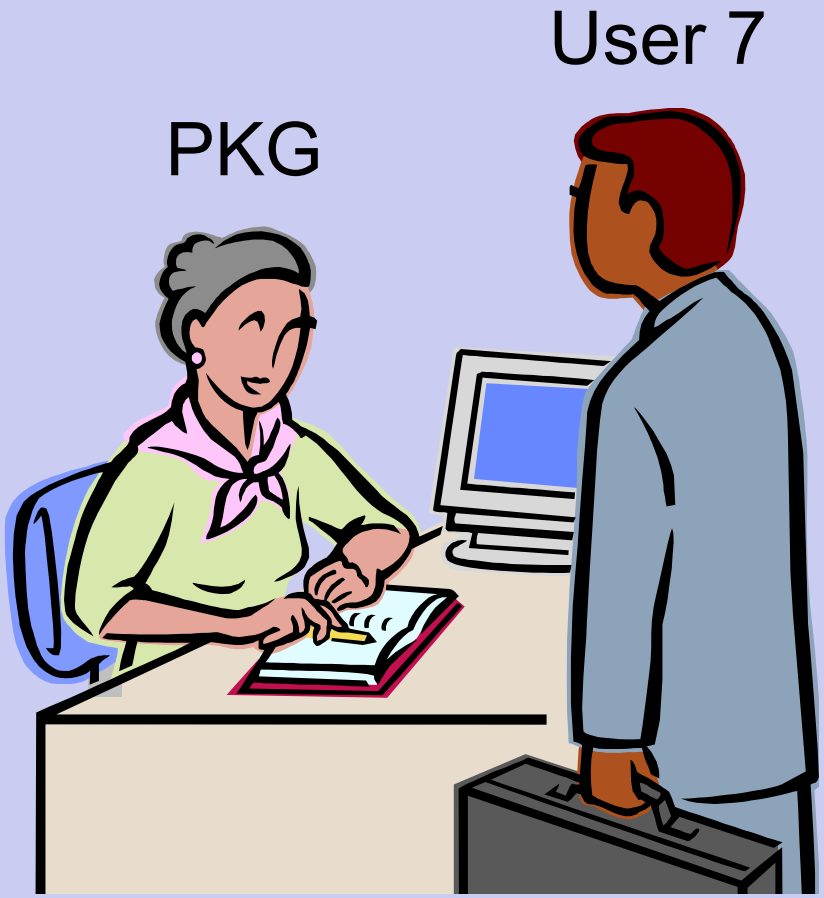
Assume there are 1000 users



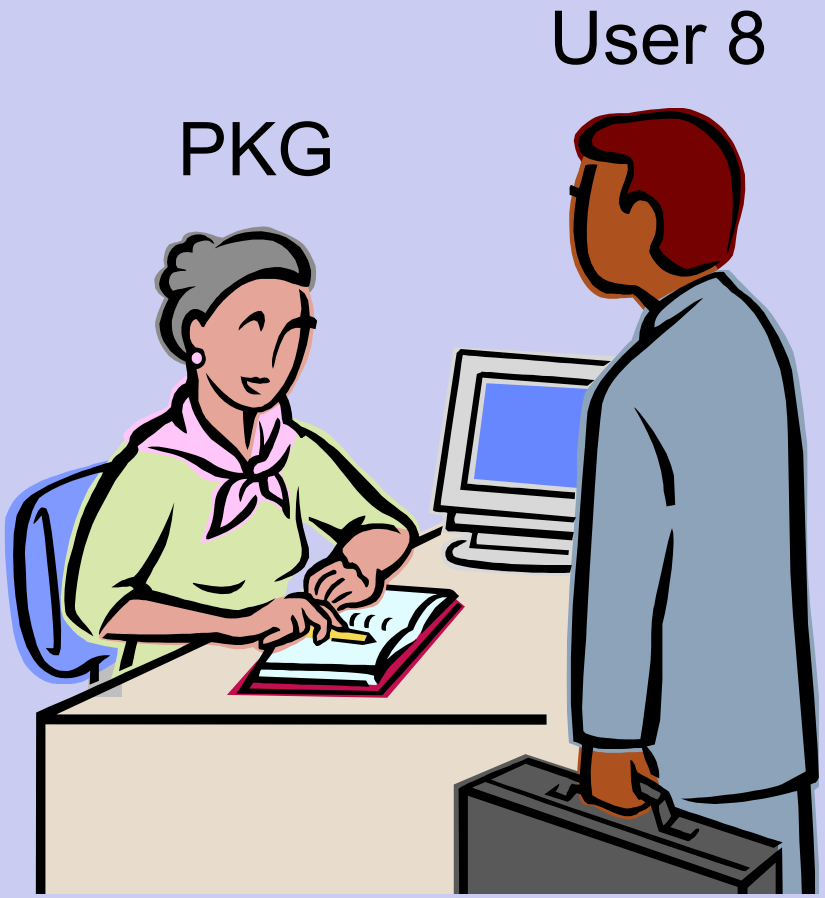
Assume there are 1000 users



Assume there are 1000 users

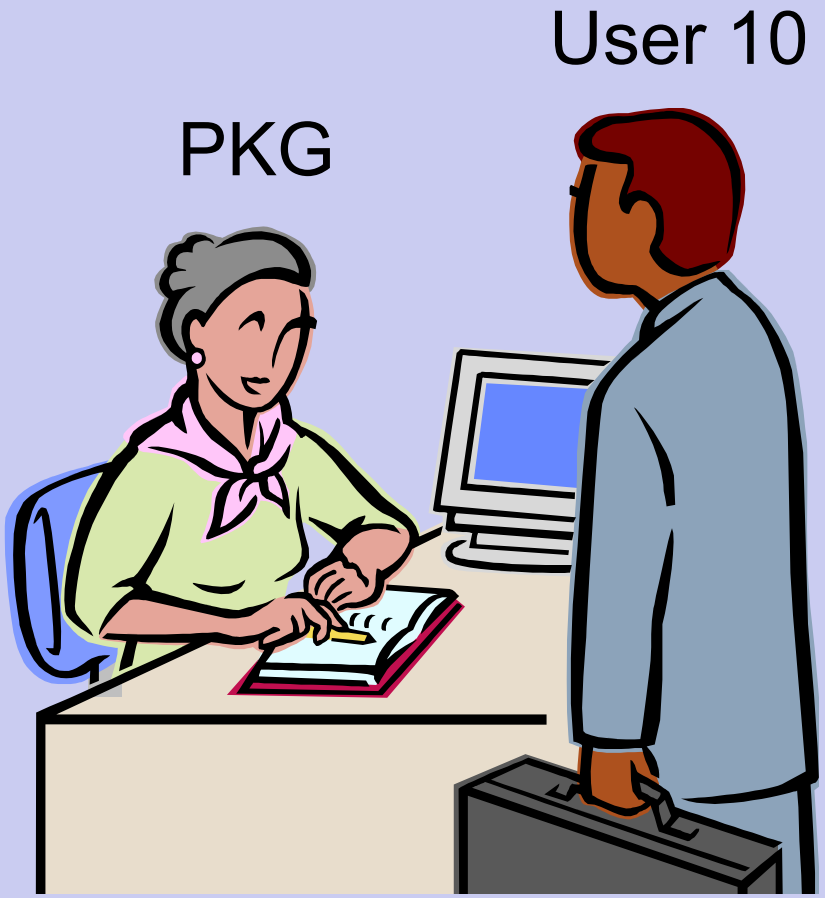


Assume there are 1000 users

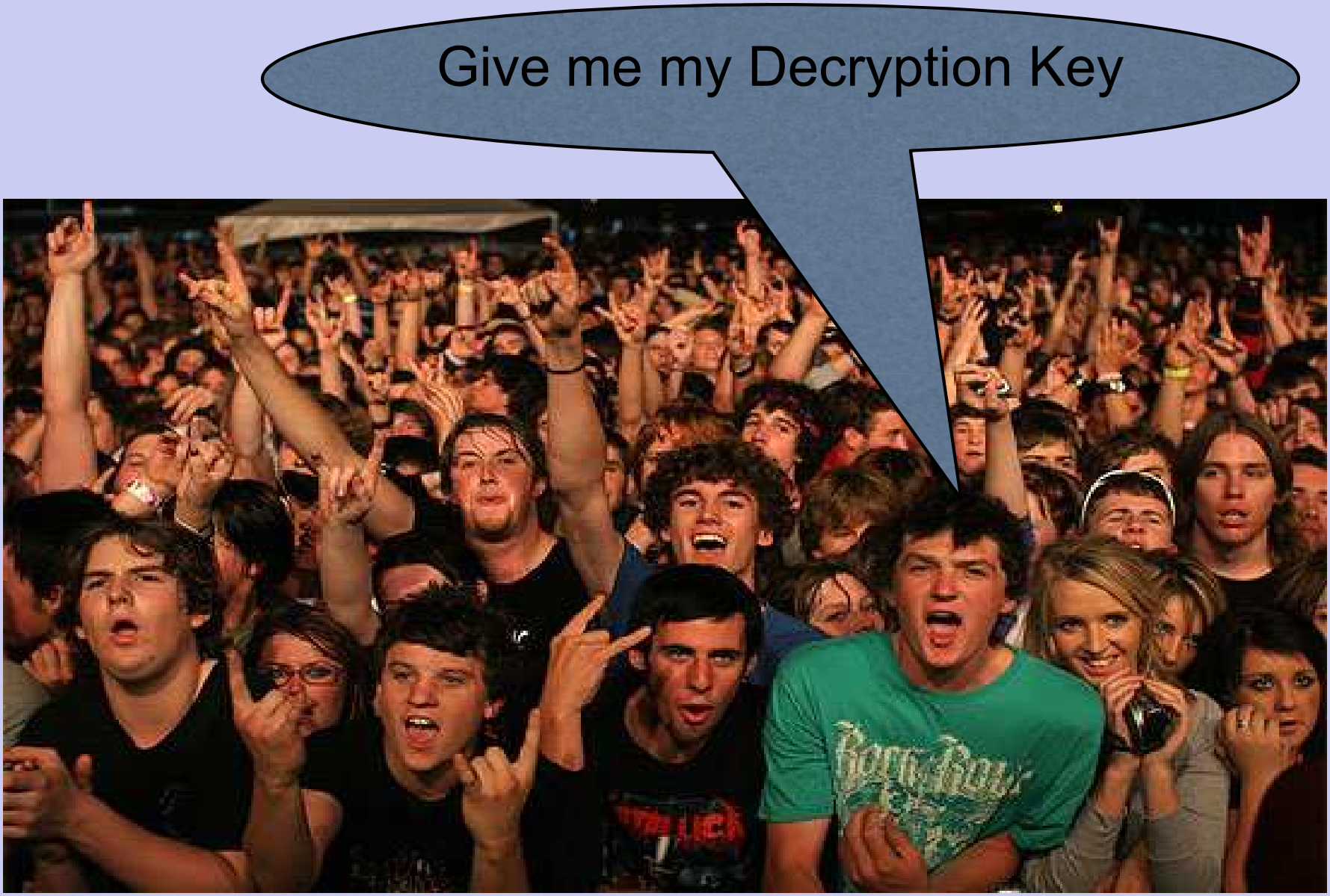


Assume there are 1000 users

Assume there are 1000 users



Assume there are 1000 users



Our Contributions

- We define a new primitive, Revocable IBE, and its security.
- We propose an efficient Revocable IBE construction, where the PKG needs only to do work logarithmic in the number of users.
- We prove security of our scheme based on the Decisional Bilinear Diffie-Hellman assumption.

Thanks!

@ CCS