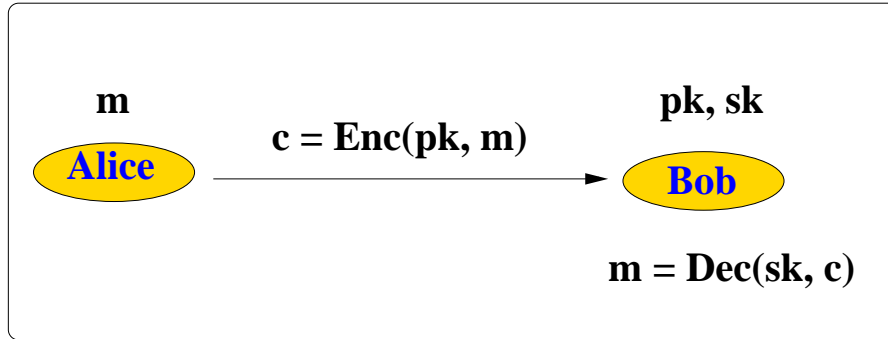


Functional Encryption (Introduction)

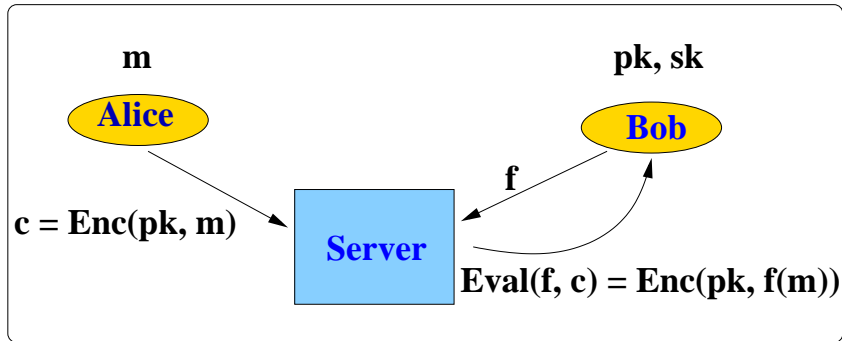
Public Key Encryption (PKE)



Drawback:

- Decryption is “all” or “nothing” affair!

Homomorphic Encryption (HE)



Drawback:

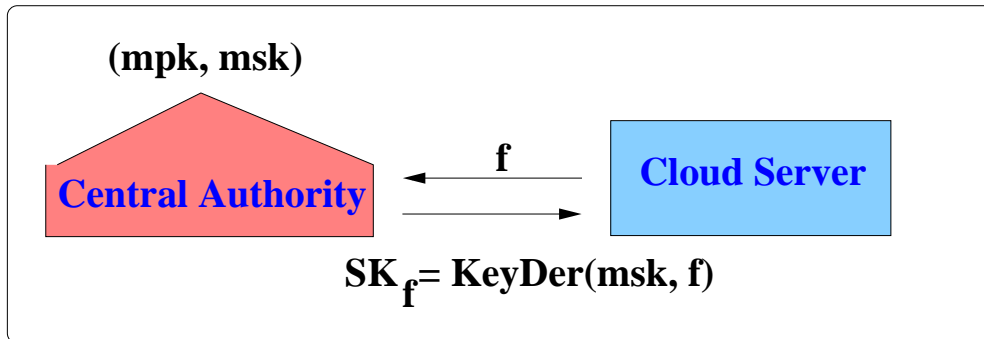
- Interaction with Bob!

Example

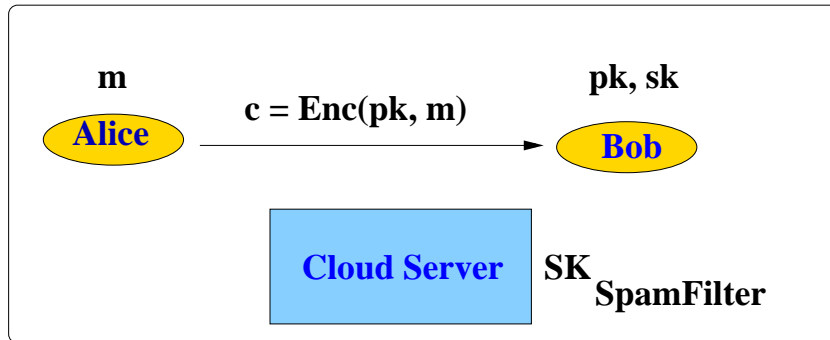
- f is $+$ operator, $c_1 = \text{Enc}(\text{pk}, m_1)$ and $c_2 = \text{Enc}(\text{pk}, m_2)$
 $\text{Eval}(f, c_1, c_2) = \text{Enc}(\text{pk}, f(m_1, m_2)) = \text{Enc}(\text{pk}, m_1 + m_2)$
- Useful to outsource private computations (cloud computing)
- **Partially homomorphic cryptosystems** - RSA, ElGamal, GM, Paillier
- **Fully homomorphic encryption** - supports arbitrary computation on ciphertexts (lattice-based cryptography)

Functional Encryption (FE)

(Delegates decryption capabilities)



Functional Encryption (FE)



if $\text{Eval}(SK_{\text{SpamFilter}}, c) = \text{True}$
then “Move to the Spam Folder”

Advantages

- Decryption does not require interaction with Bob!
- Fine-Grained Access Control of Decryption Capabilities!

FE: Credit Card Transaction Alert

- Credit Card Transaction Alert (SK_{Alert})

if $Eval(SK_{Alert}, c) = \text{True}$
then “Fire an Alarm”

Alert: Transactions over Rs. 1.0 Lakhs

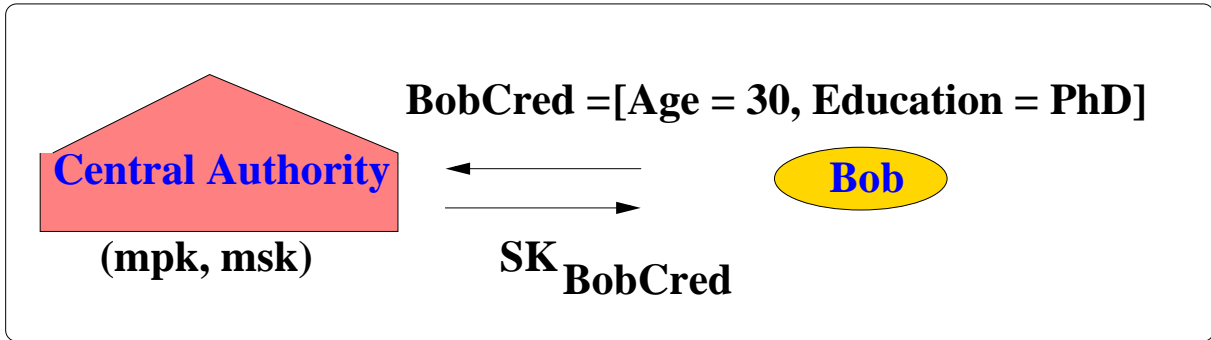
FE: Credit Card Fraud Investigation

- Credit Card Fraud Investigation ($SK_{f_{\text{Auditing}}}$)

if $\text{Eval}(SK_{f_{\text{Auditing}}}, c) = \text{True}$
then “Fire an Alarm”

f_{Auditing} : Transactions over Rs. 1.0 Lakhs which took place in November and originated from Kolkata.

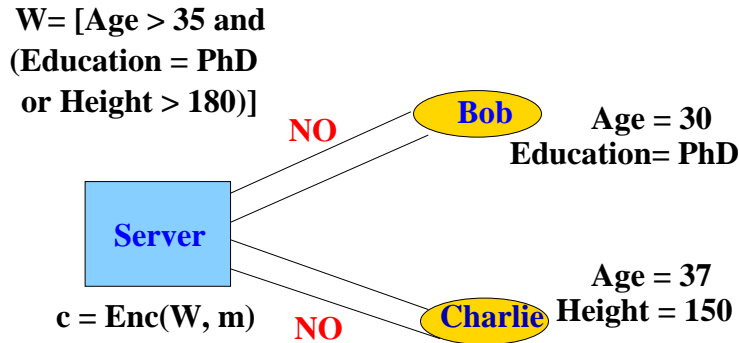
FE: Online dating



Bob has specific attributes and will receive a secret key that can only decrypt profiles for which the attributes match the dating preferences.

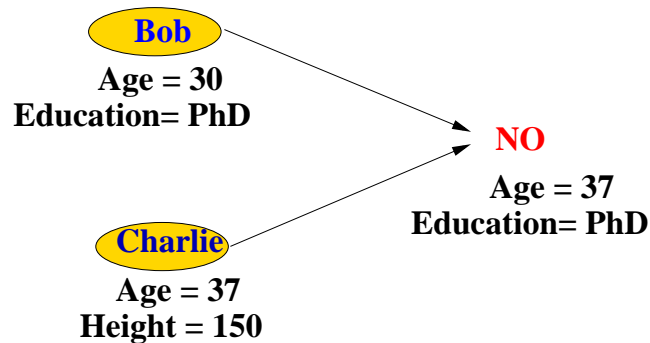
FE: Online dating

- profile m is encrypted under the dating preferences (access structure) $W = [\text{Age} > 35 \text{ and Education} = \text{PhD or Height} > 180]$



FE: Online dating - Collusion Resistance

- profile m is encrypted under the dating preferences (access structure) $W = [\text{Age} > 35 \text{ and } (\text{Education} = \text{PhD or Height} > 180)]$
- primitive should withstand collusion attack



Current Lines of Work

- Efficient functional encryption for access control
- Functional encryption for all circuits
- Efficient constructions for expressive functionalities

FE: Definition

A Functional Encryption (FE) scheme for the functionality \mathcal{F} consists of the following algorithms:

$$(\text{mpk}, \text{msk}) \longleftarrow \text{Setup}(1^\lambda, \mathcal{F})$$

$$\text{SK}_f \longleftarrow \text{KeyDer}(\text{msk}, f)$$

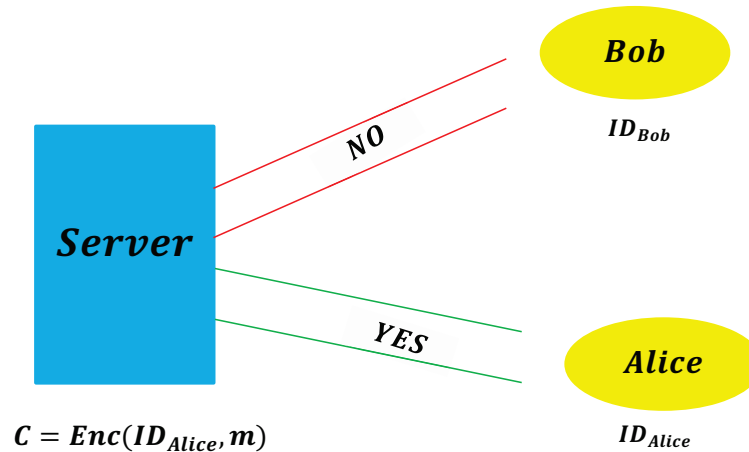
$$\text{CT} \longleftarrow \text{Enc}(\text{mpk}, m)$$

$$f(m) \longleftarrow \text{Dec}(\text{SK}_f, \text{CT})$$

Examples of Functionalities

- (Hierarchical) Identity-Based Encryption
- Fuzzy Identity-Based Encryption
- Attribute-Based Encryption
- Predicate Encryption
- etc.

Identity-Based Encryption (IBE)



Generalized Hierarchical IBE (HIBE)

