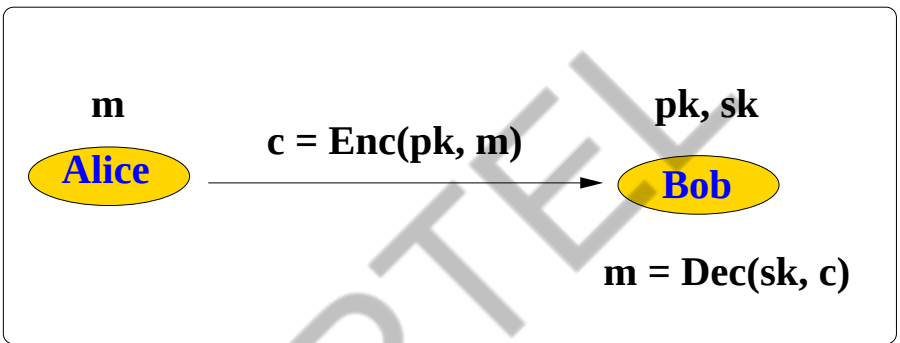
Functional Encryption (Introduction)

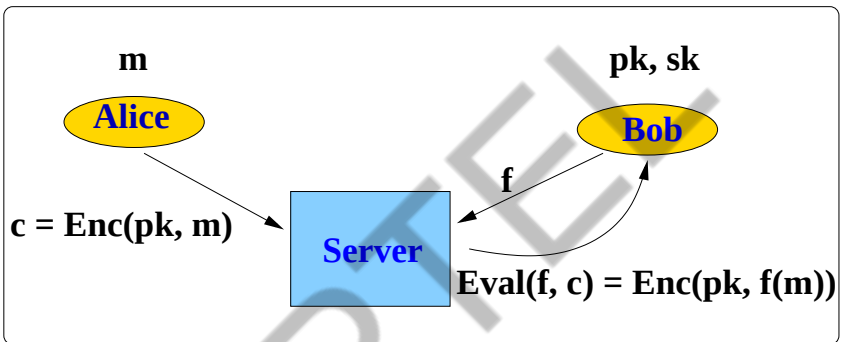
Public Key Encryption (PKE)



Drawback:

- Decryption is "all" or "nothing" affair!

Homomorphic Encryption (HE)



Drawback:

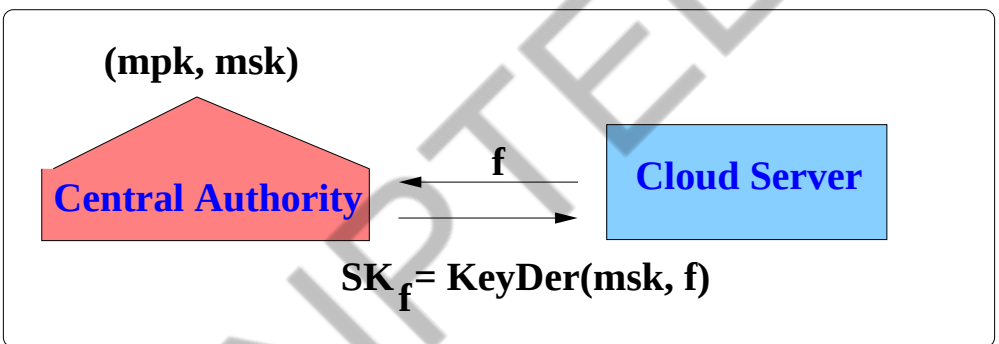
- Interaction with Bob!

Example

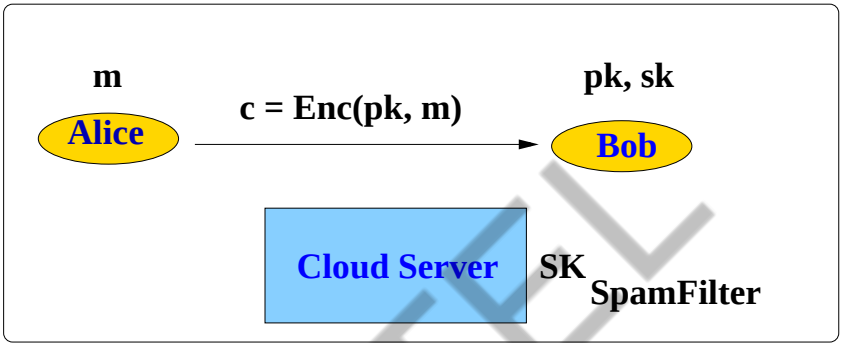
- f is + operator, $c_1 = \mathsf{Enc}(\mathsf{pk}, m_1)$ and $c_2 = \mathsf{Enc}(\mathsf{pk}, m_2)$ $\mathsf{Eval}(f, c_1, c_2) = \mathsf{Enc}(\mathsf{pk}, f(m_1, m_2)) = \mathsf{Enc}(\mathsf{pk}, m_1 + m_2)$
- Useful to outsource private computations (cloud computing)
- **Partially homomorphic cryptosystems**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

Functional Encryption (FE)

(Delegates decryption capabilities)



Functional Encryption (FE)



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

Advantages

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

FE: Credit Card Transaction Alert

- Credit Card Tranaction Alert ($\mathsf{SK}_{\mathsf{Alert}}$)

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

Alert: Transactions over Rs. 1.0 Lakhs

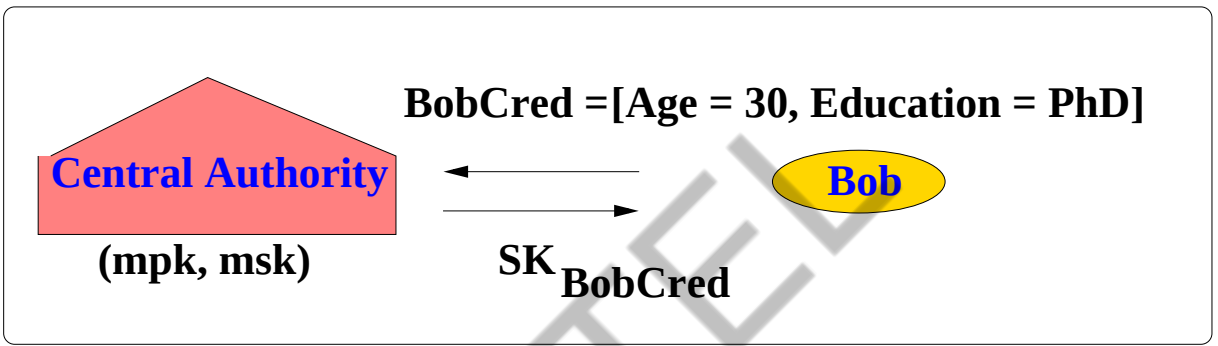
FE: Credit Card Fraud Investigation

- Credit Card Fraud Investigation ($\mathsf{SK}_{f_{\mathsf{Auditing}}}$)

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

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

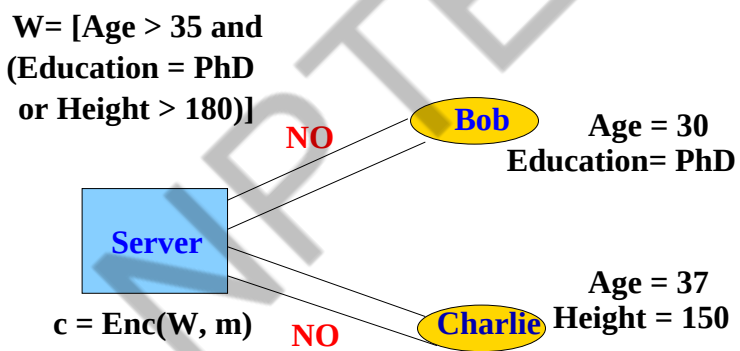
FE: Online dating



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

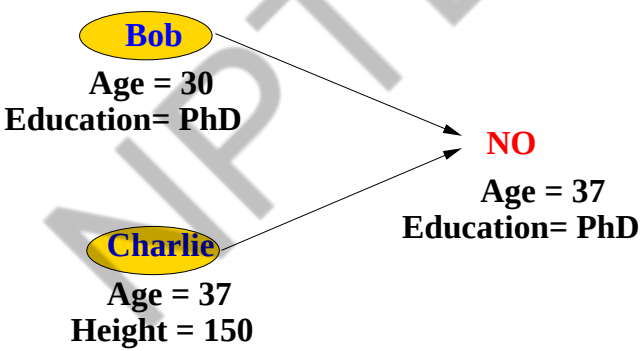
FE: Online dating

- profile m is encrypted under the dating preferences (access structure) $W = [$ Age > 35 and Education $=$ 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:

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

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

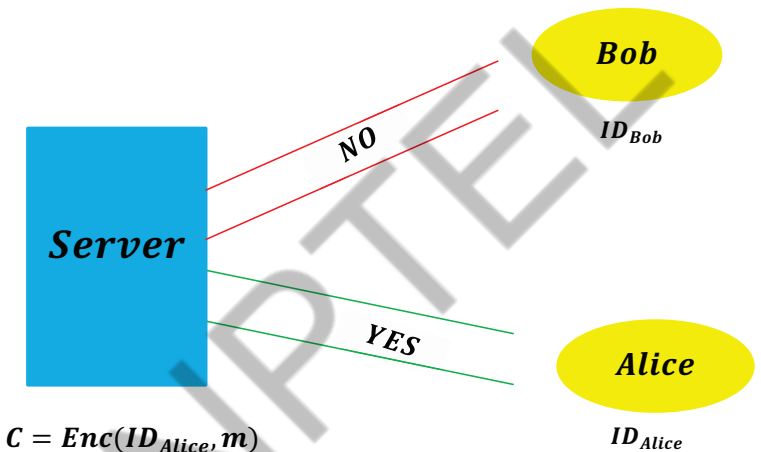
$$\mathsf{CT} \longleftarrow \mathsf{Enc}(\mathsf{mpk}, m)$$

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

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)