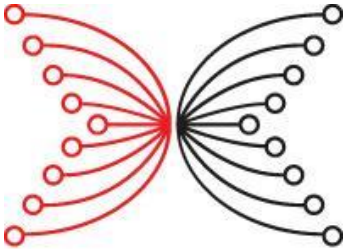
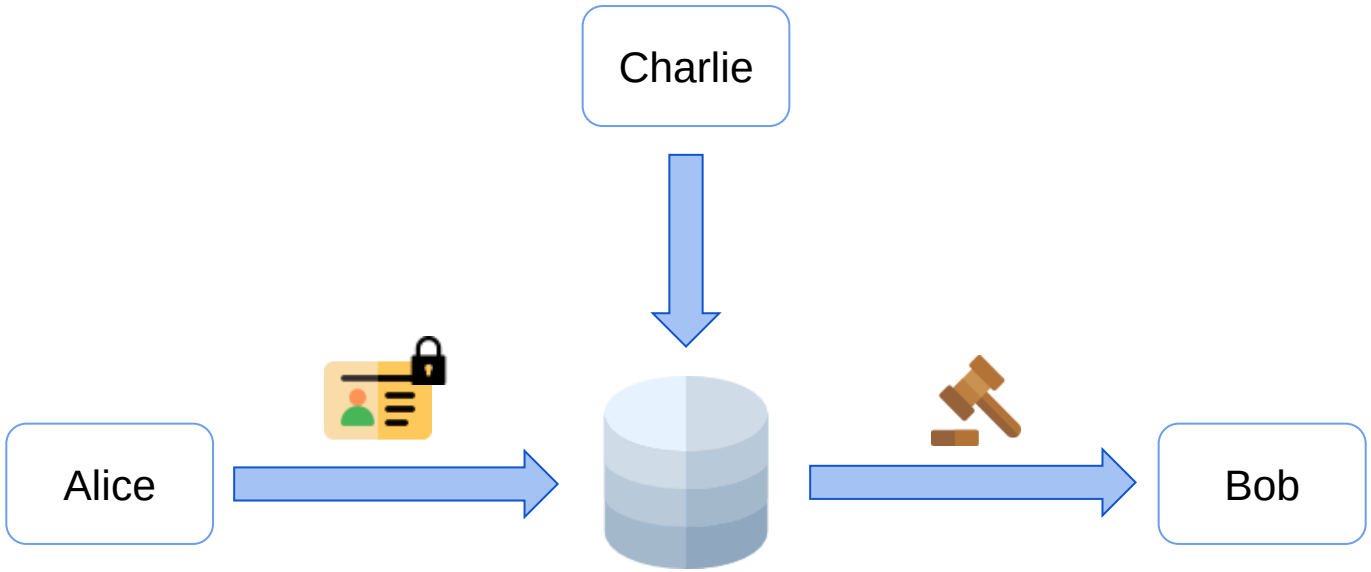
Consistency for Functional Encryption

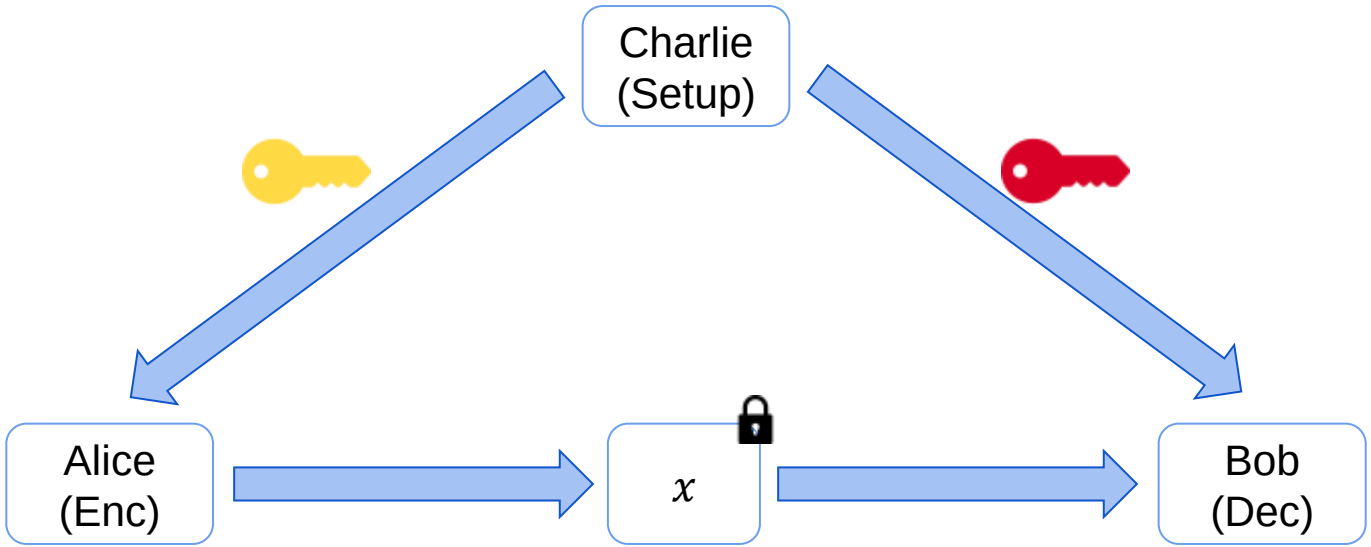
Christian Badertscher, Aggelos Kiayias,
Markulf Kohlweiss, Hendrik Waldner



Motivation

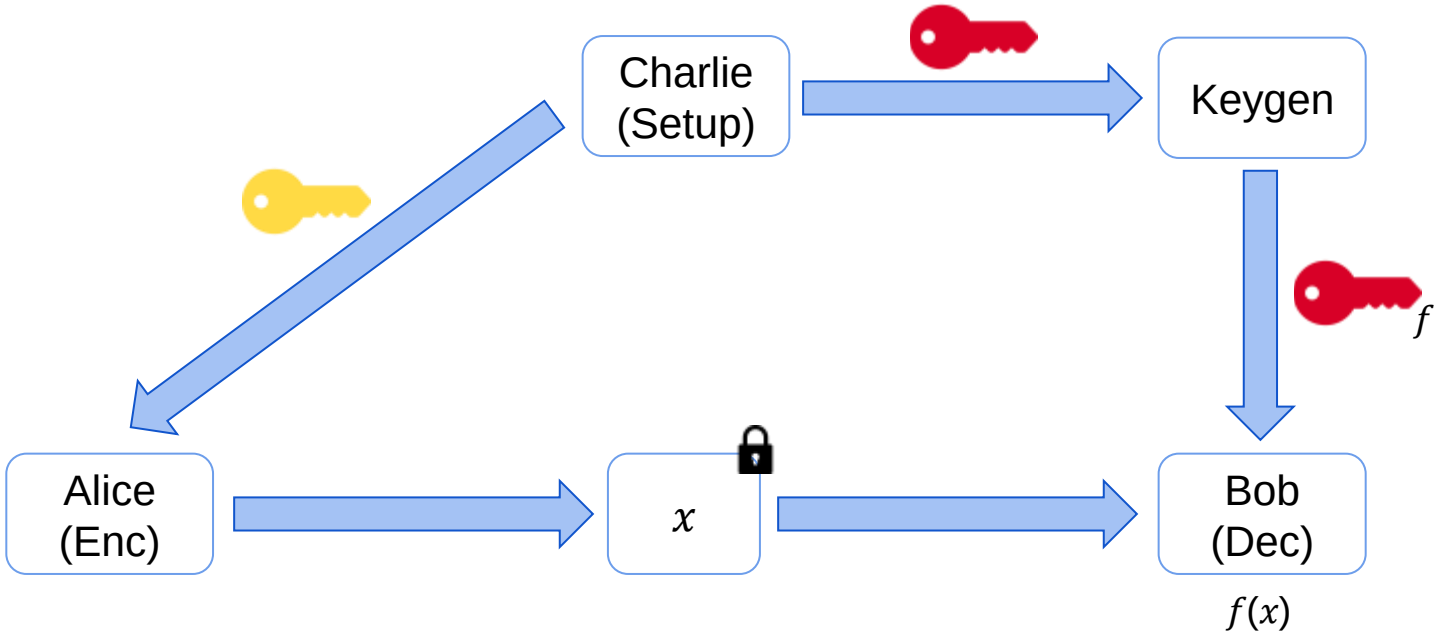


Public Key Encryption [DH76]



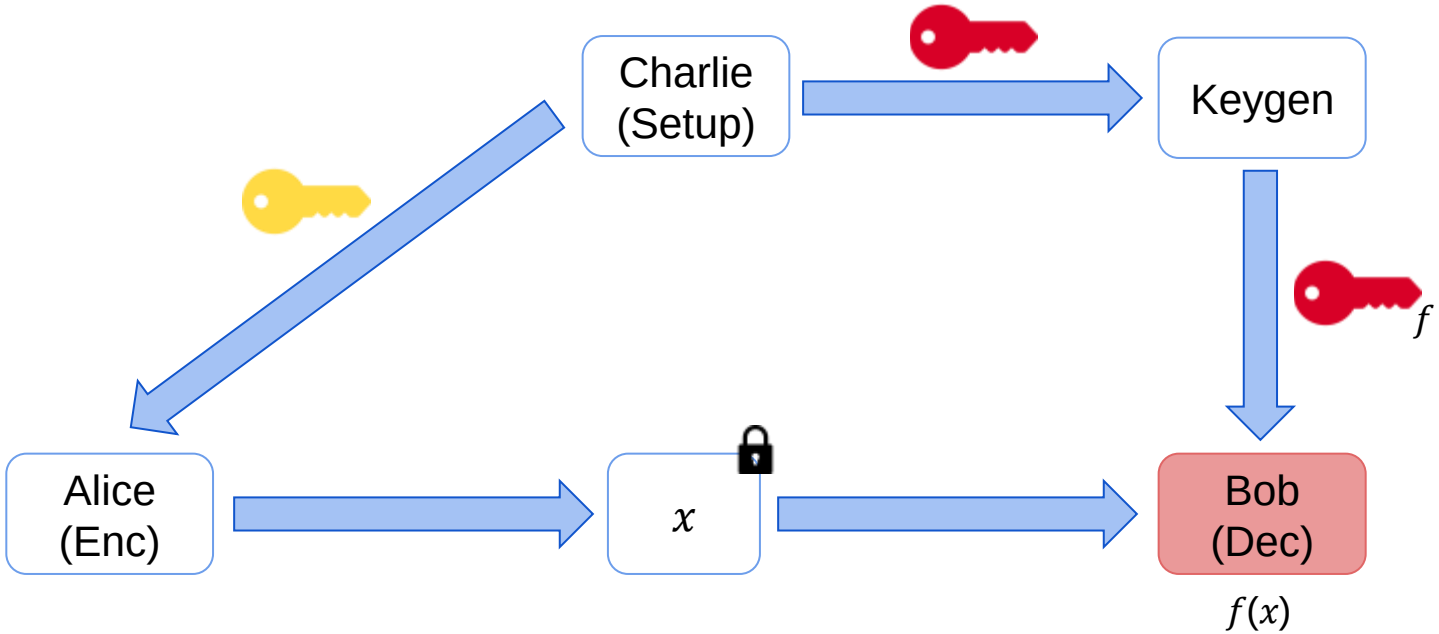
No fine grained access control

Functional Encryption [BSW11]



Desired Access Control!

Functional Encryption [BSW11]



Security (Malicious Bob)

$b \leftarrow \{0,1\}$

(mpk,msk)←Setup

mpk

$sk_f \leftarrow Keygen(msk, f)$

f

sk_f

(x_0, x_1)

$ct \leftarrow Enc(mpk, x_b)$

ct

$sk_f \leftarrow Keygen(msk, f)$

f

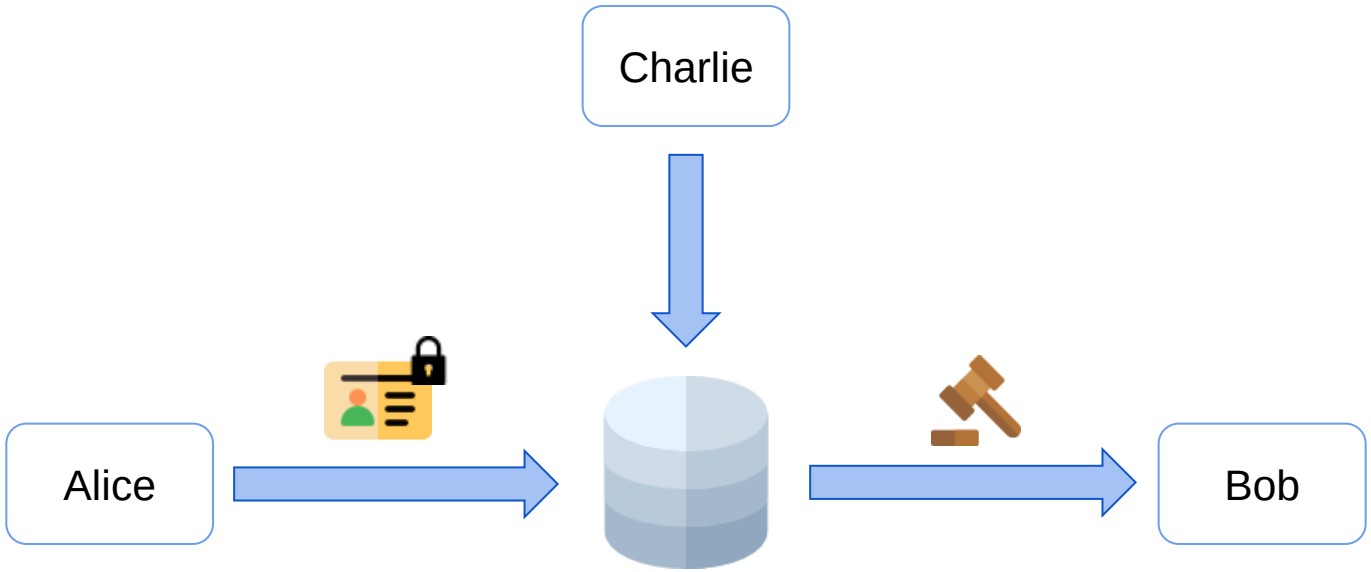
sk_f

$\forall f: f(x_0)=f(x_1)$

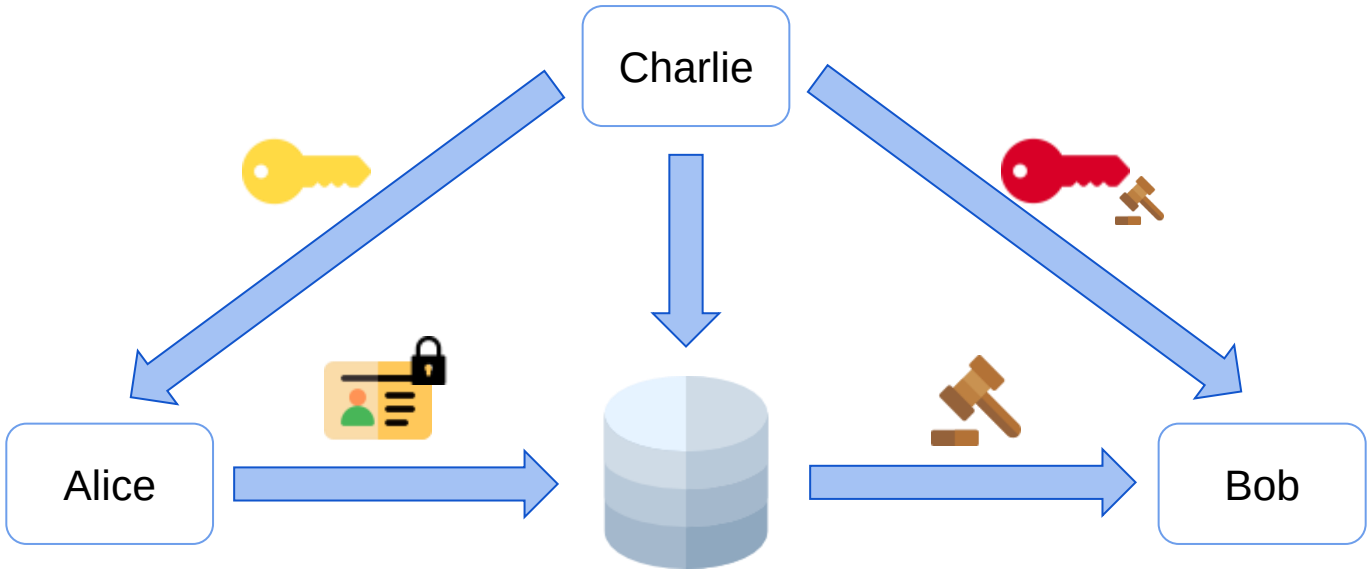
b'

If $b=b'$ Adversary wins

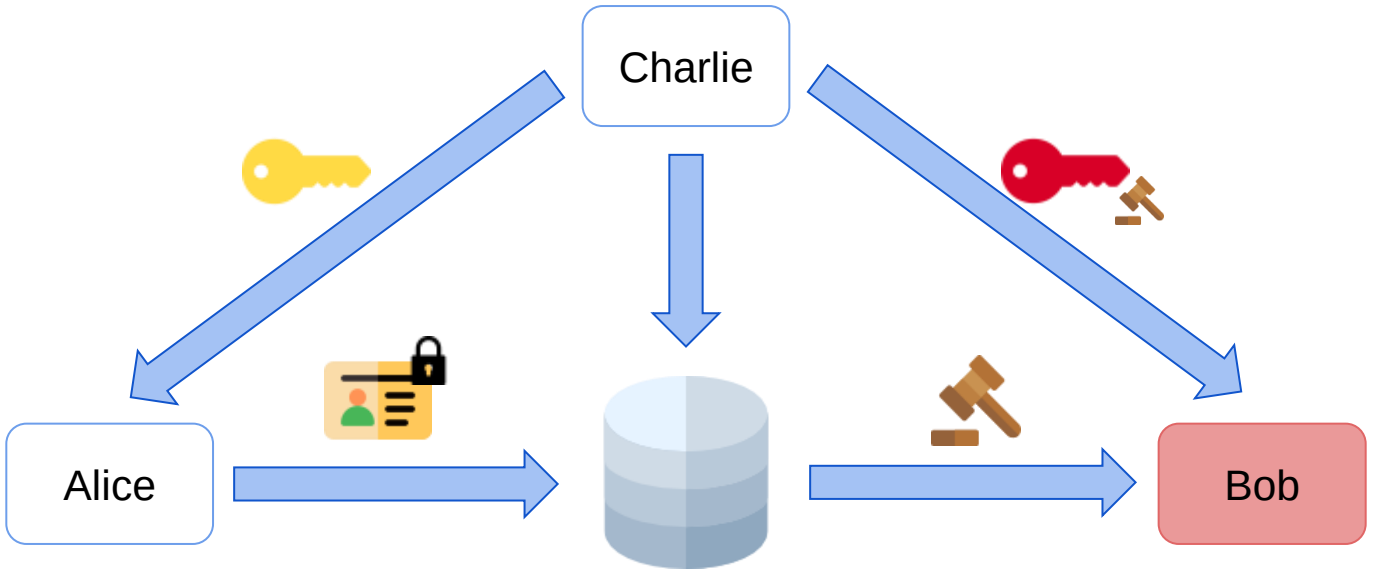
Motivation



Motivation

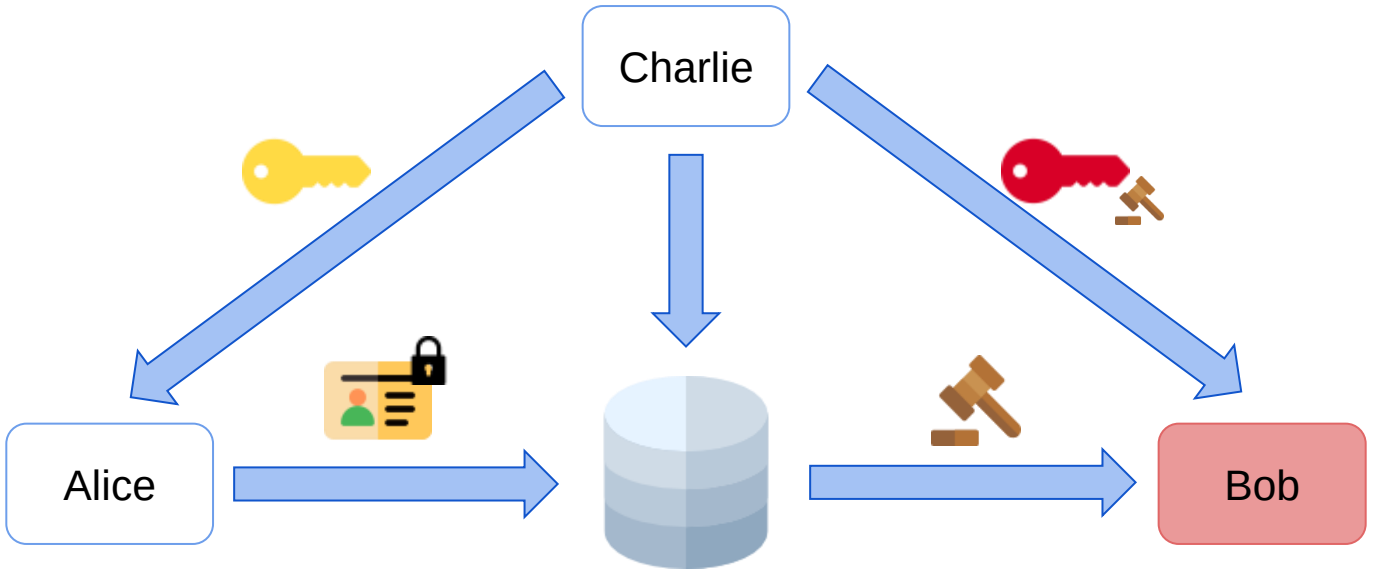


Motivation (Malicious Bob)



Cannot learn more than what is specified by

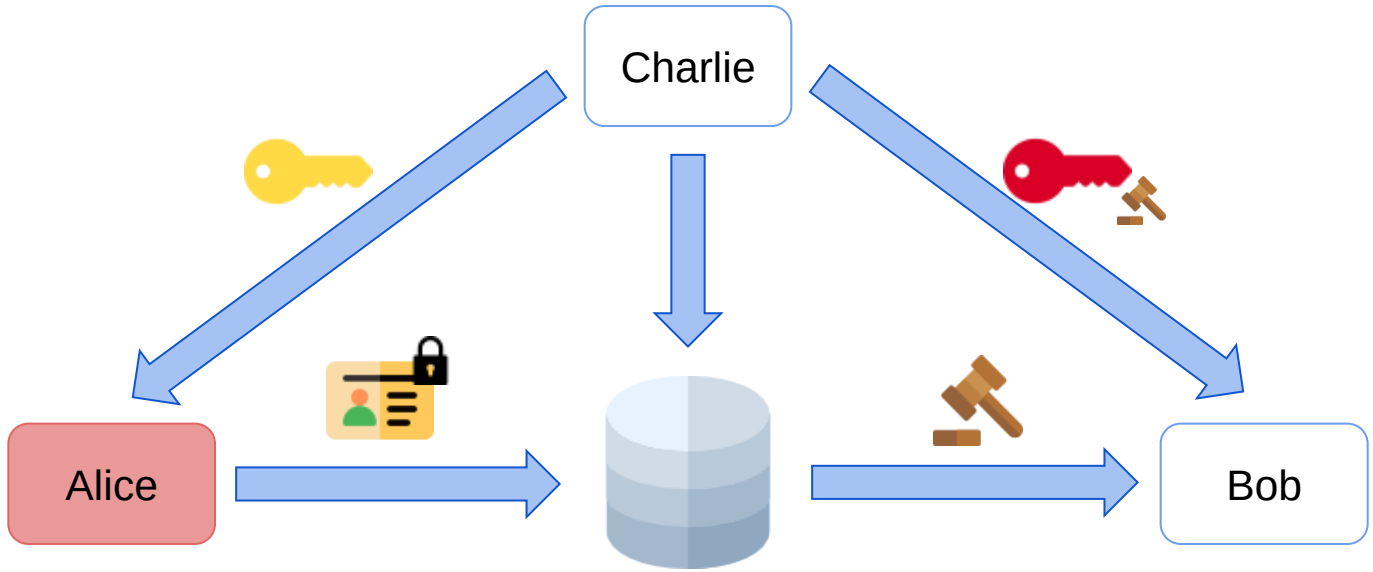
Motivation (Malicious Bob)



Cannot learn more than what is specified by

What about the other parties?

Motivation (Malicious Alice)



Cannot create a misclassifying

Input Consistency (Malicious Alice)

(mpk,msk)←Setup

mpk

sk_f←Keygen(msk,f)

f

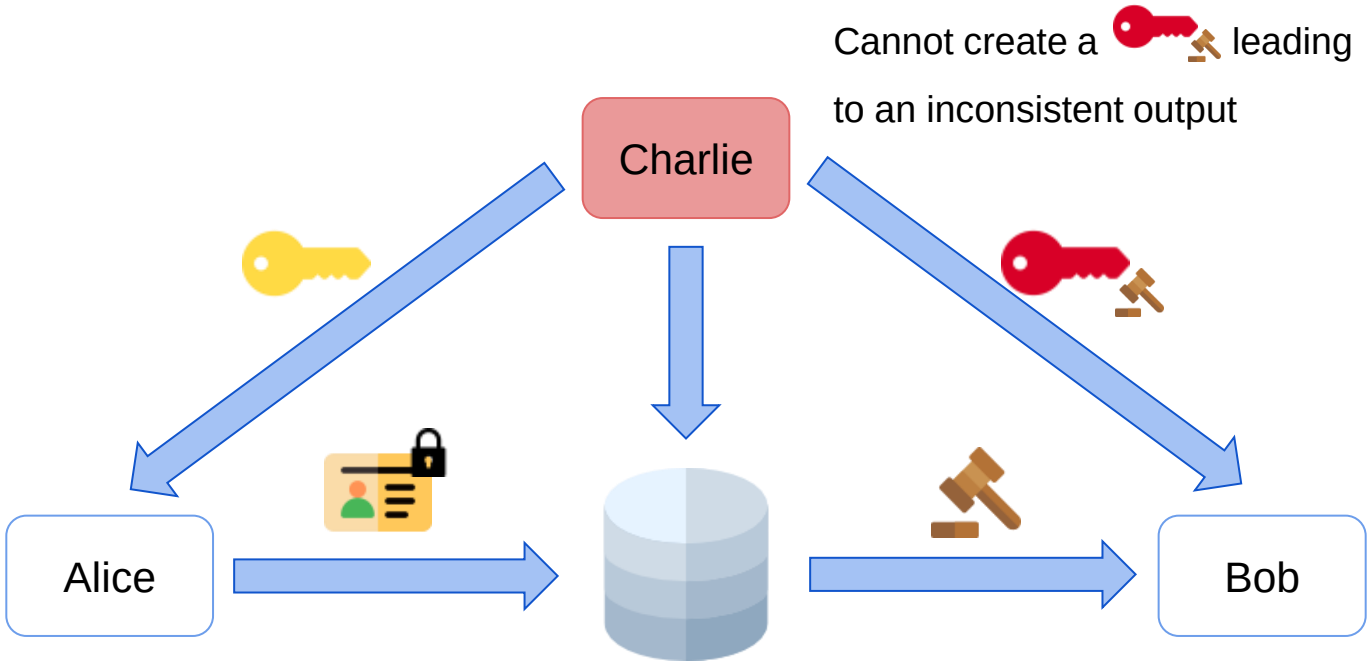
sk_f

y_i=Dec(mpk,f_i,sk_f,ct)

ct

If $\bigcap_i f_i^{-1}(y_i)=\emptyset$
Adversary wins

Motivation (Malicious Charlie)



Setup Consistency (Malicious Charlie)

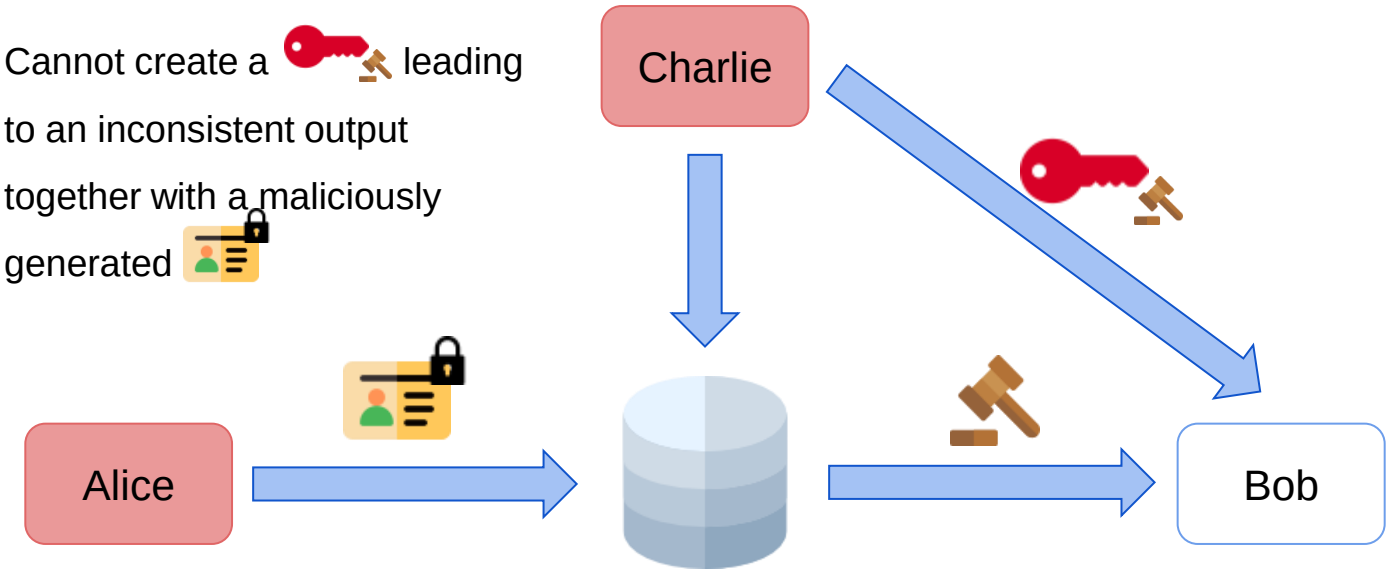
$(\mathsf{mpk}, f, \mathsf{sk}, x_1, x_2)$

$\mathsf{ct}_1 \leftarrow \mathsf{Enc}(\mathsf{mpk}, x_1)$
$\mathsf{ct}_2 \leftarrow \mathsf{Enc}(\mathsf{mpk}, x_2)$

$y_1 = \mathsf{Dec}(\mathsf{mpk}, f, \mathsf{sk}, \mathsf{ct}_1)$
$y_2 = \mathsf{Dec}(\mathsf{mpk}, f, \mathsf{sk}, \mathsf{ct}_2)$

If $y_1 \neq f(x_1) \vee y_2 \neq f(x_2)$
Adversary wins

Motivation (Malicious Alice & Charlie)



Strong Input Consistency (Malicious Alice & Charlie)

$(\mathsf{mpk},(f_i,\mathsf{sk}_i)_i,\mathsf{ct}_1,\mathsf{ct}_2)$

$y_{1,i}=\mathsf{Dec}(\mathsf{mpk},f_i,\mathsf{sk}_i,\mathsf{ct}_1)$
$y_{2,i}=\mathsf{Dec}(\mathsf{mpk},f_i,\mathsf{sk}_i,\mathsf{ct}_2)$

If $\bigcap_i f_i^{-1}(y_{1,i})=\emptyset \vee \bigcap_i f_i^{-1}(y_{2,i})=\emptyset$
Adversary wins

Further Results

- Relationship between Consistency and Security
- Analysis of existing Functional Encryption schemes
- Compilers for any Functional Encryption scheme

  ⇒ Based on NIZKs and NIWIs [BGJS16]

- Analysis in the UC Framework [MM15]

Thank You!

Questions?