Functional Encryption: Introduction & Recent Advances

Gil Segev

Hebrew University

What’s Functional Encryption?

Public-Key Encryption

$\mathrm{Enc}(pk, m)$ $\longrightarrow$

Alice

Bob's public key pk

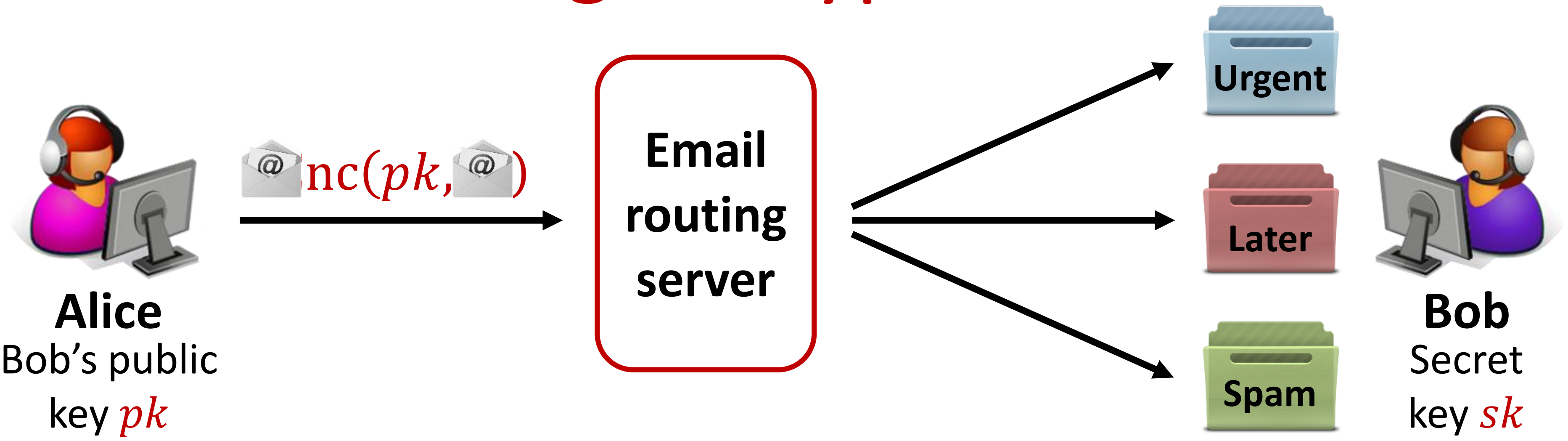
Bob

Secret key sk

"All-or-nothing" approach:

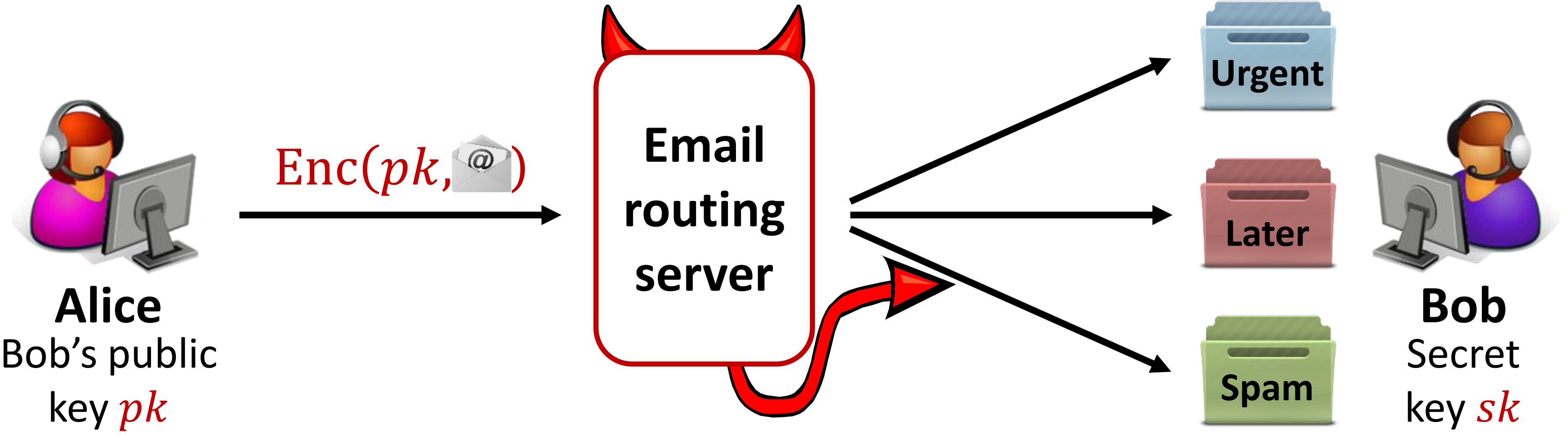
- Without sk: The ciphertext is useless
- With sk: Can recover the message

Filtering Encrypted Email



$$F : \text{Emails} \rightarrow \{\text{Urgent}, \text{Later}, \text{Spam}\}$$

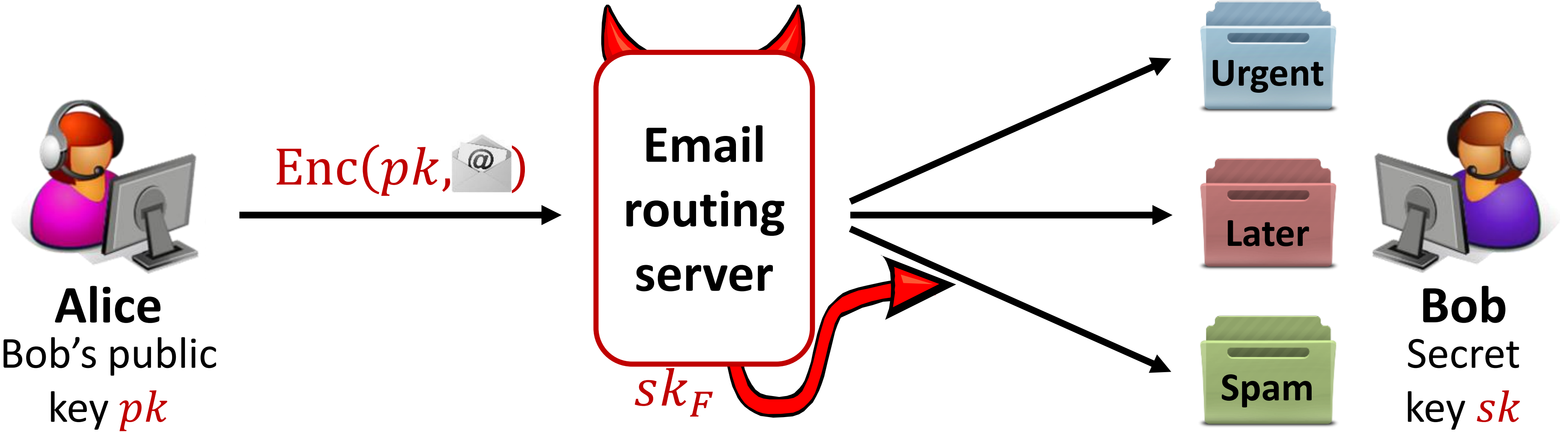
Filtering Encrypted Email



Can the server filter encrypted emails?

- Without sk: The server is useless
- With sk: The server can decrypt and apply F

Filtering Encrypted Email

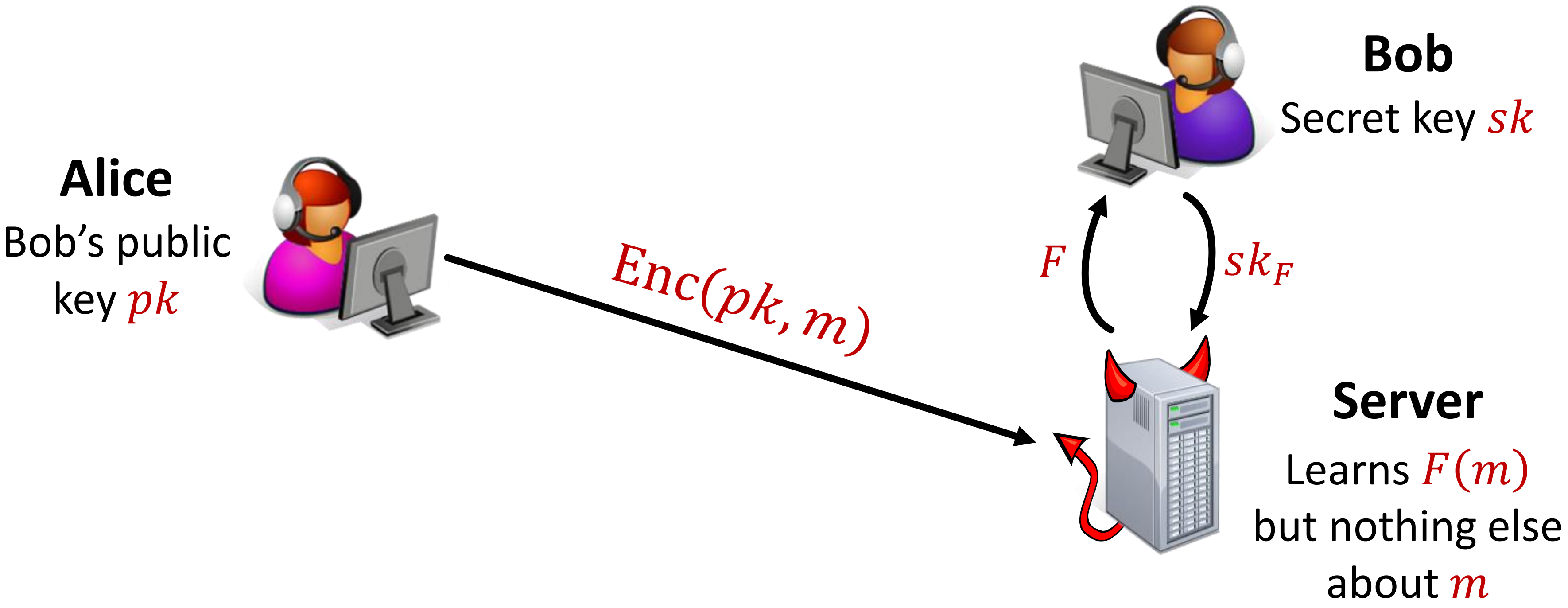


Solution: Functional Encryption

- Bob issues the server a "restricted" key sk_F
- Given $\mathrm{Enc}(pk, m)$ the server can compute $F(m)$ but nothing else!

Functional Encryption

[Sahai-Waters ‘05]



This Talk

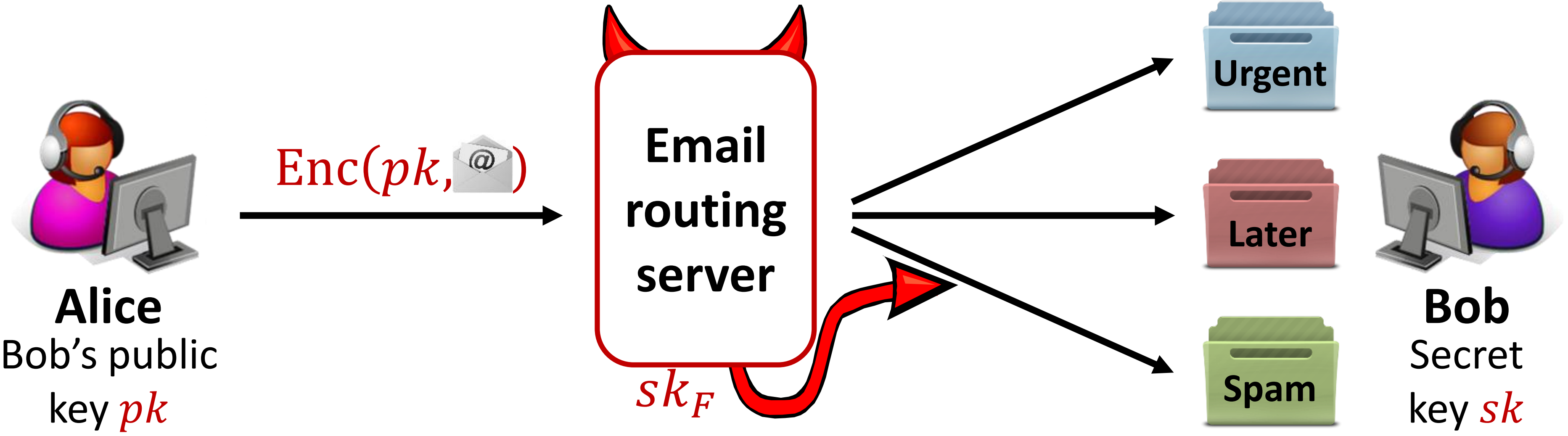
- **Direct applications**

- **The security of functional encryption**

- **The road so far: From public-key to functional encryption**

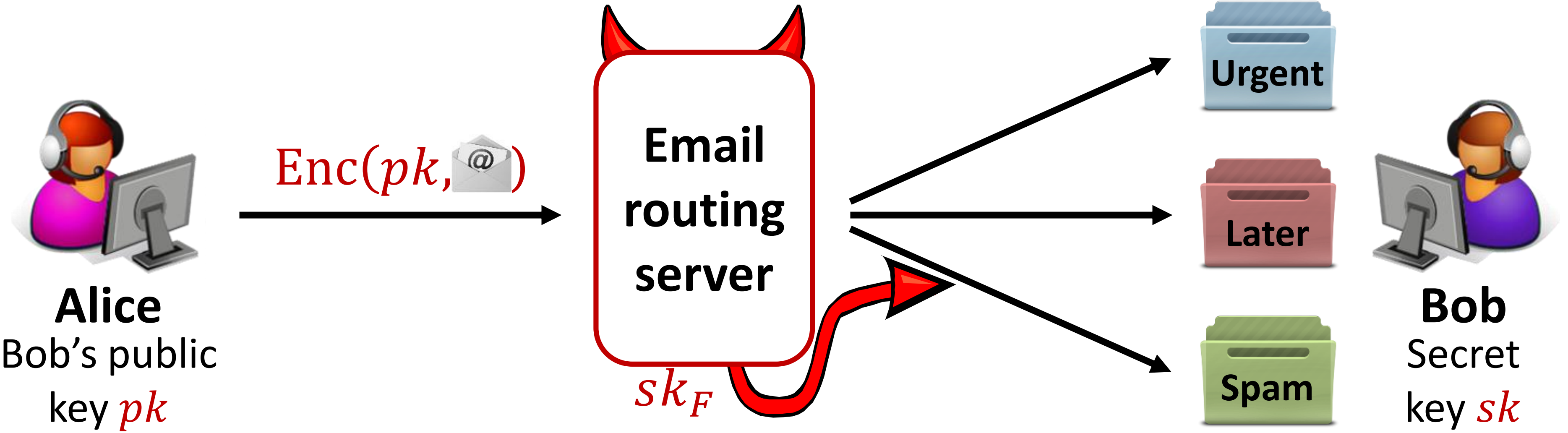
- **The road ahead**

Filtering Encrypted Email



$$F: \text{Emails} \rightarrow \{\text{Urgent}, \text{Later}, \text{Spam}\}$$

Filtering Encrypted Email

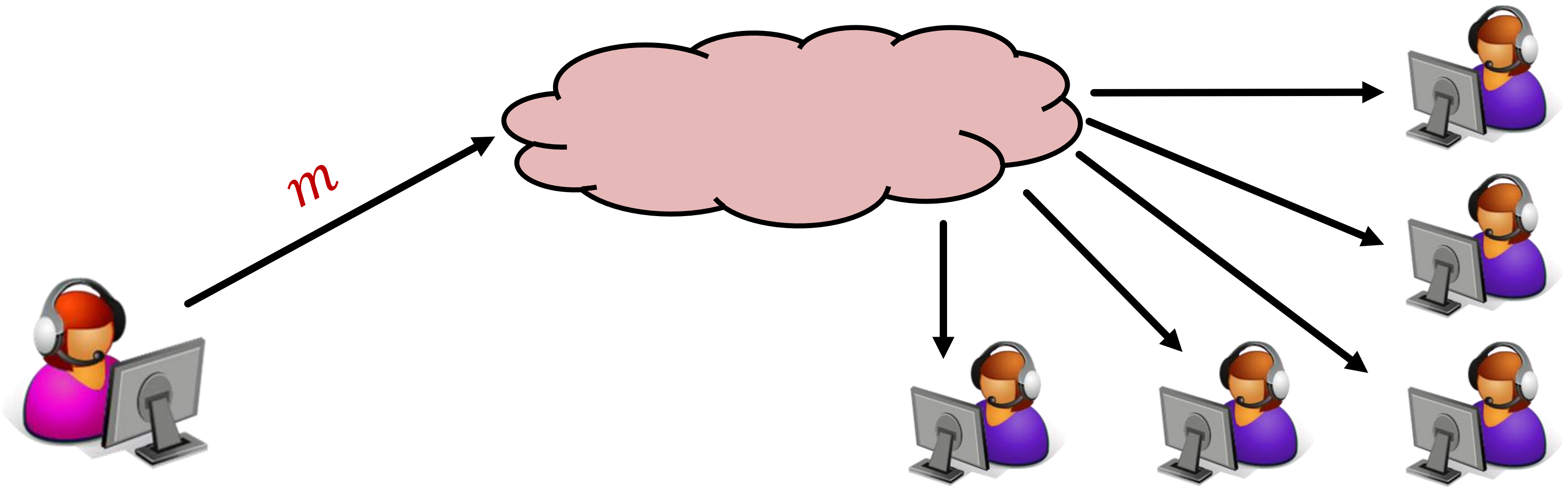


More generally: Remote access to encrypted data

- Enable user-side encryption!
- …

OneDrive
Google Drive
Dropbox

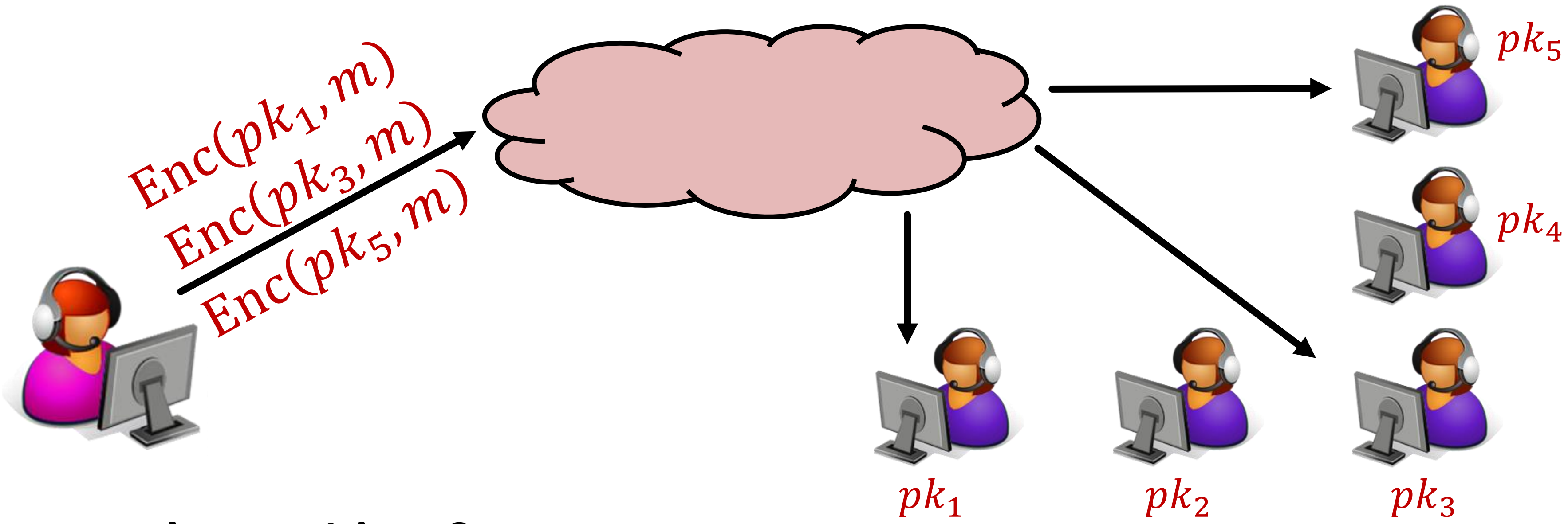
Expressive Access Control



Who should be allowed access?

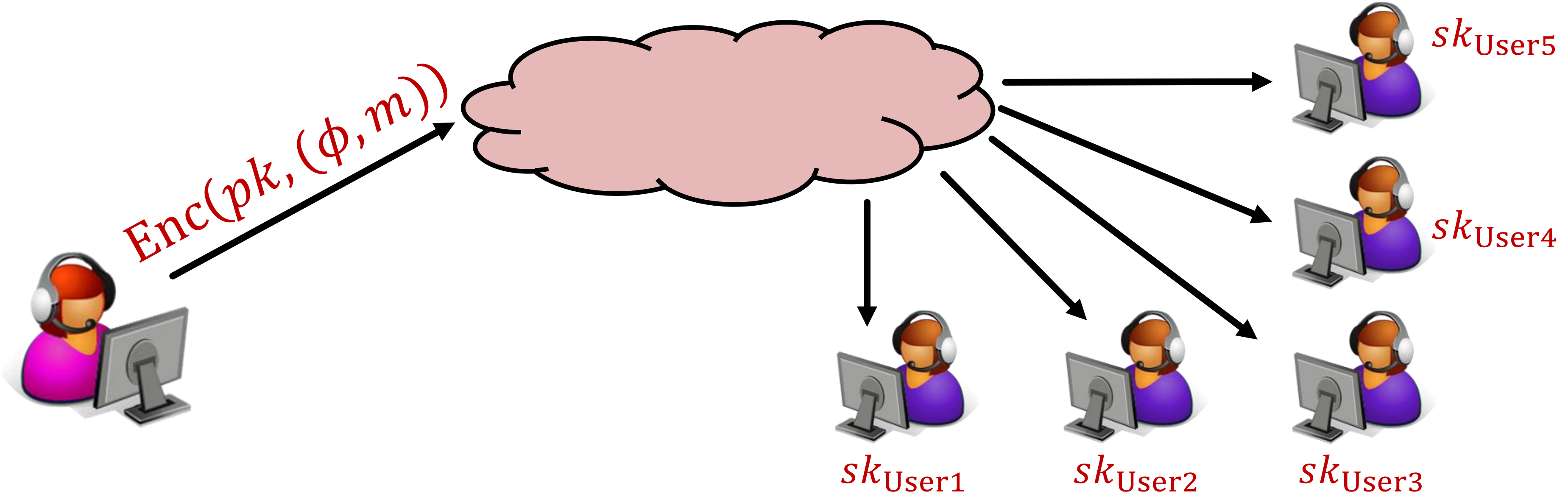
$$\left(\begin{pmatrix}\text{CEO's}\\ \text{Office}\end{pmatrix} \vee \begin{pmatrix}\text{Marketing \&}\\ \text{Location} = \text{CA}\end{pmatrix}\right) \bigwedge (\text{Age} \geq 24)$$

Expressive Access Control



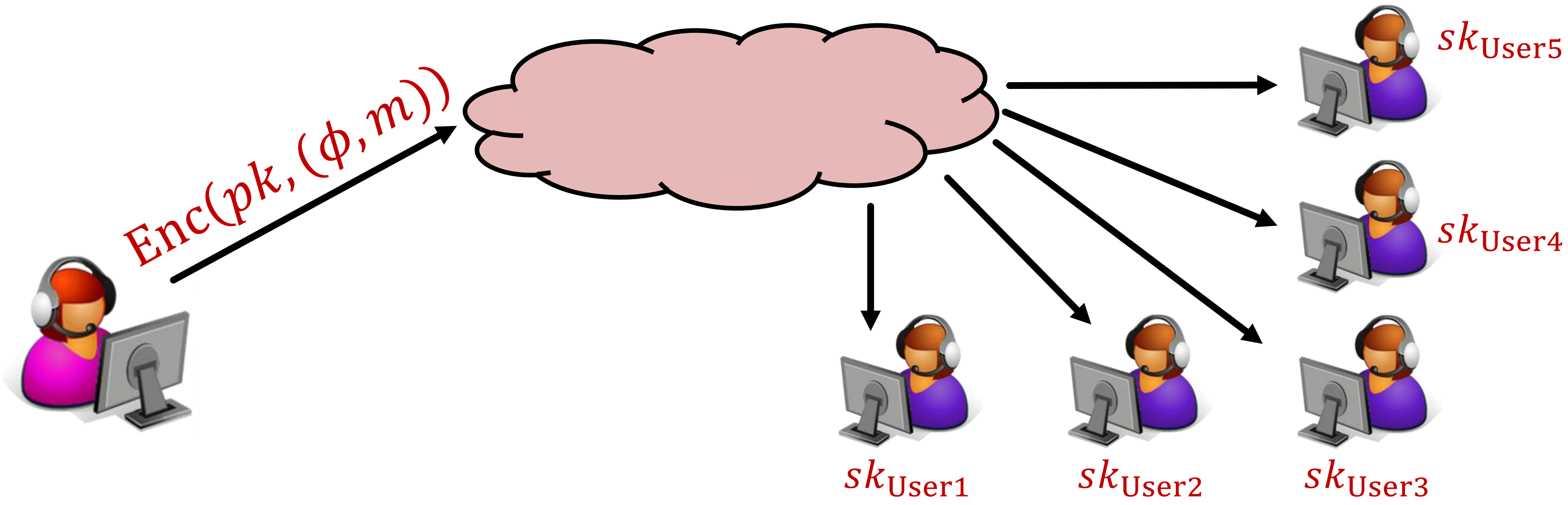
Any better ideas?

Expressive Access Control



$$\phi = \left(\begin{pmatrix} \text{CEO's} \\ \text{Office} \end{pmatrix} \vee \begin{pmatrix} \text{Marketing \&} \\ \text{Location} = \text{CA} \end{pmatrix} \right) \bigwedge (\text{Age} \geq 24)$$

Expressive Access Control

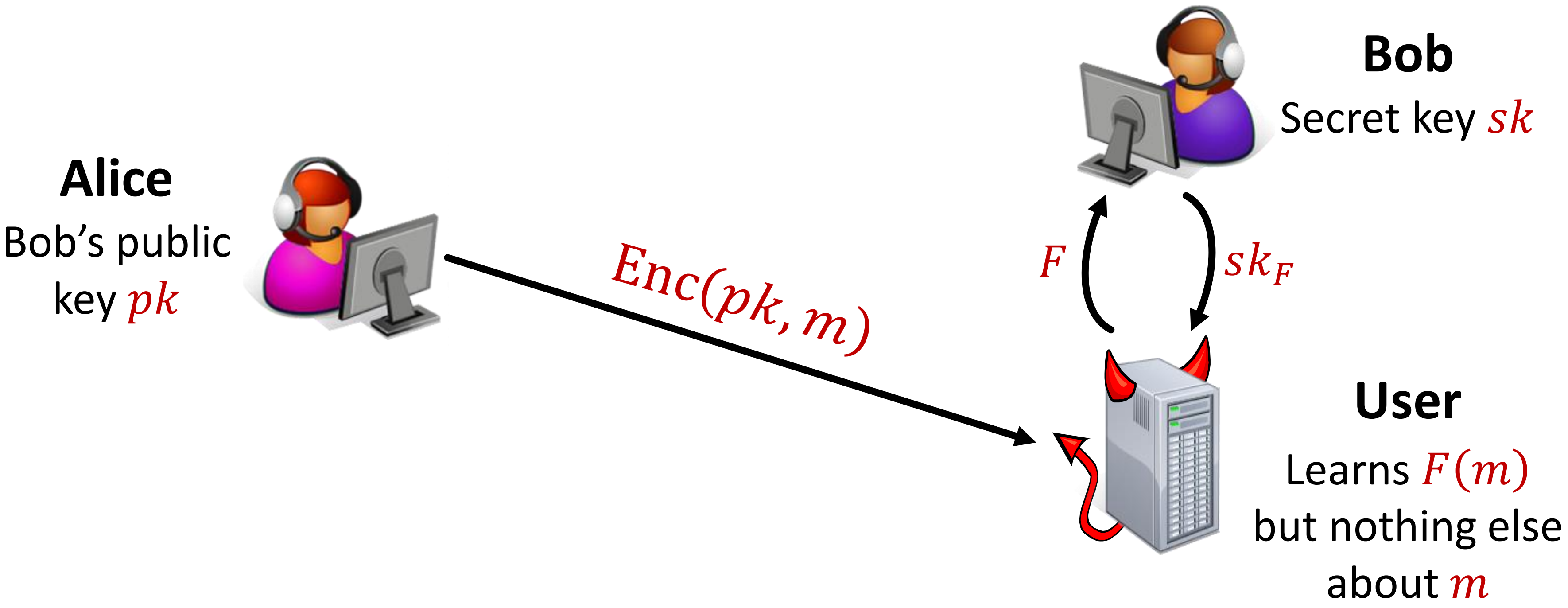


$$F_{\mathrm{User}}(\phi,m)=\begin{cases} m & \text{if } \phi(\mathrm{User})=1 \\ \perp & \text{otherwise} \end{cases}$$

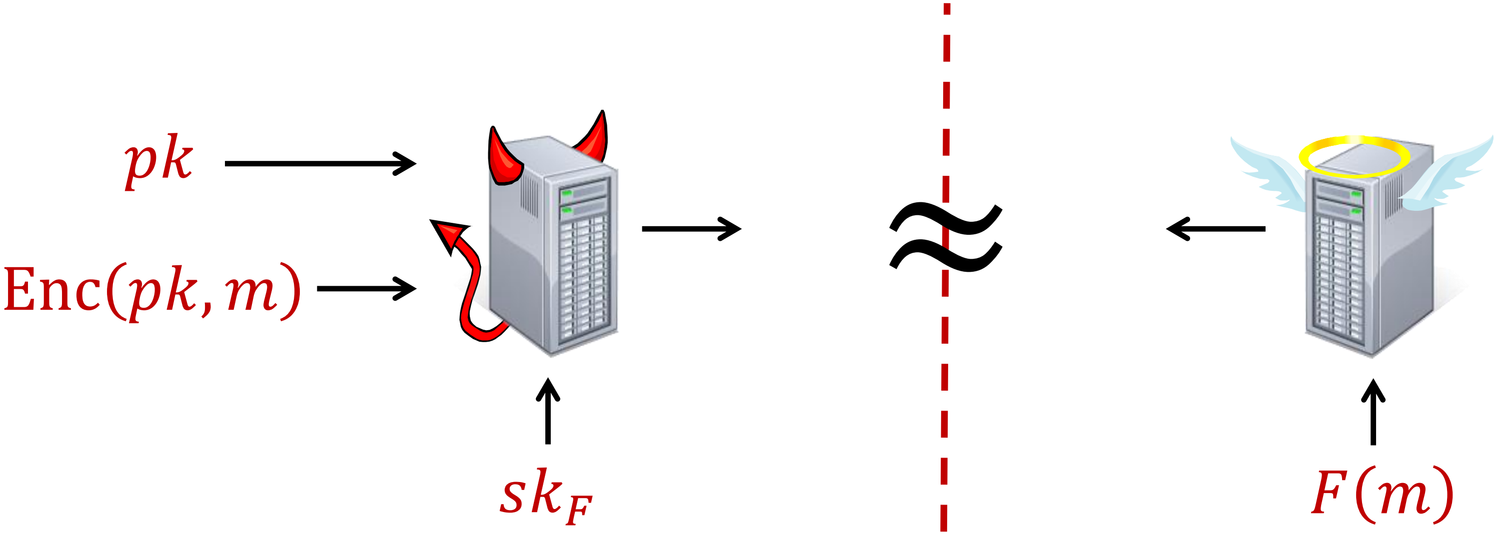
This Talk

- **Direct applications**
- **The security of functional encryption**
- **The road so far: From public-key to functional encryption**
- **The road ahead**

What About Security?



Simulation-Based Security



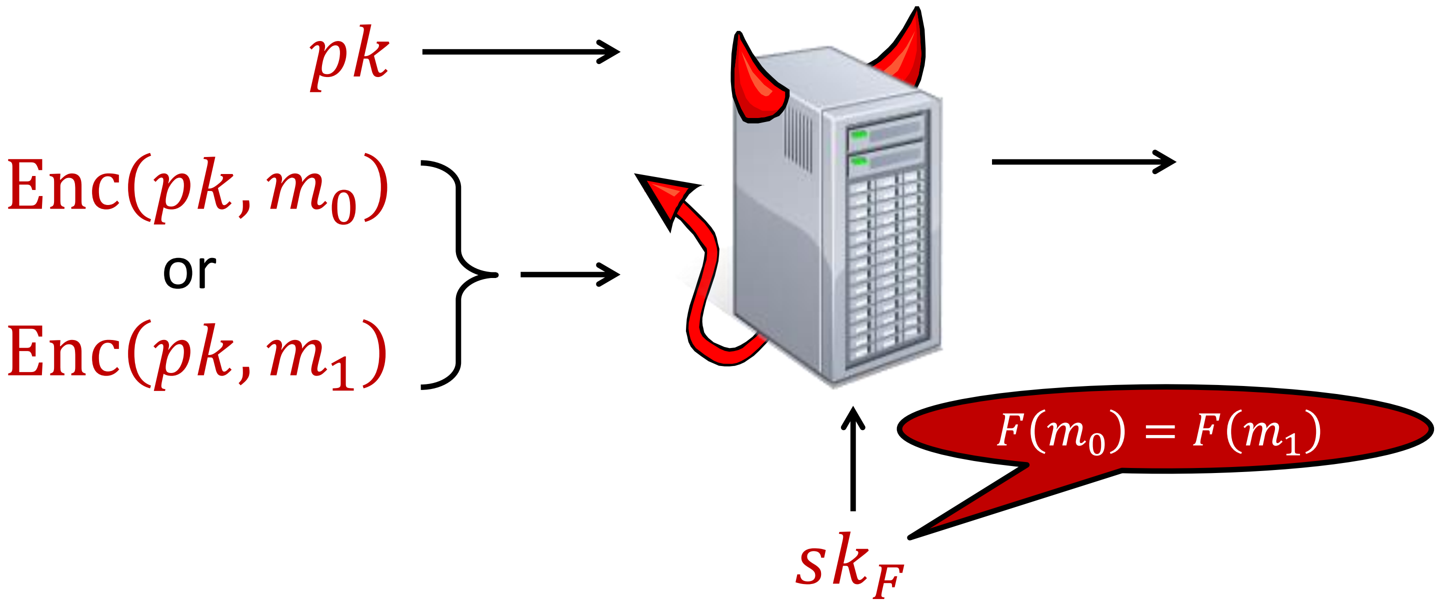
Variants:

- Random vs. selective vs. adaptive
- Bounded vs. unbounded collusions (# of keys)
- Poly-time vs. unbounded simulator
- …

Bad news [BSW11,AGVW13,…]:

Generally impossible for unbounded collusions…

Indistinguishability-Based Security



Simulation vs. Indistinguishability:

- Equivalent for non-functional encryption [GM82]
- Indistinguishability suffices for most FE applications

This Talk

- **Direct applications**
- **The security of functional encryption**
- **The road so far: From public-key to functional encryption**
- **The road ahead**

The Road So Far

Public-Key Encryption

$\xrightarrow{\mathrm{Enc}(pk, m)}$

Alice

Bob's public key pk

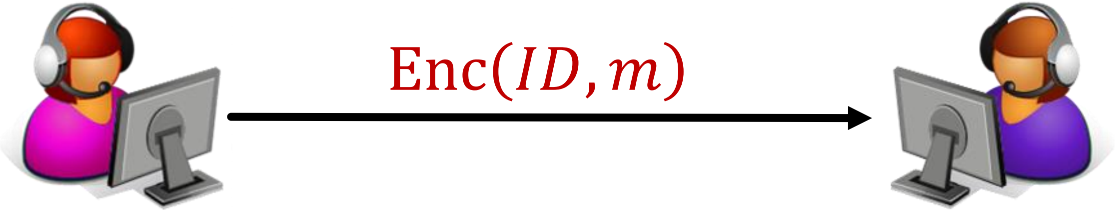
Bob

Secret key sk

Shamir (CRYPTO '84):
Can Bob's public key be an arbitrary string?

$$\boldsymbol{pk} = \text{"}\mathbf{bob@company.com}\text{"}$$

Identity-Based Encryption



Alice

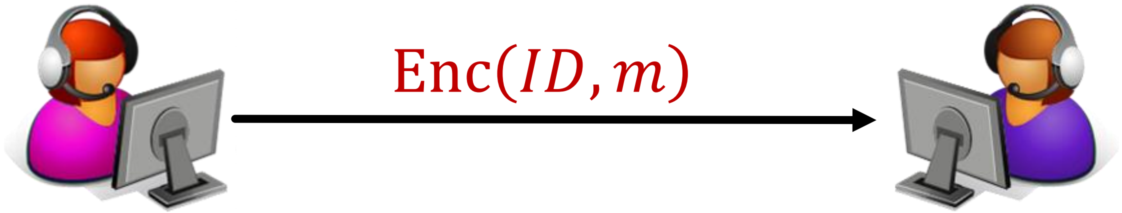
Bob's $ID = \text{"bob@company.com"}$

Bob

Secret key sk_{ID}

$$F_{ID}(x, m) = \begin{cases} m & \text{if } x = ID \\ \perp & \text{otherwise} \end{cases}$$

Identity-Based Encryption



Alice

Bob's $ID = \text{"bob@company.com"}$

Bob

Secret key sk_{ID}

Current status:

- First schemes in 2001 [BF01,C01]
- By now a variety of known schemes based on standard assumptions
- Generalizations: Hierarchical IBE [HL02,GS02], fuzzy IBE [SW05],…
- Better security: Anonymity [BF01], leakage resilience [ADNSWW10], function privacy [BRS13],…

The Road So Far

Public-Key Encryption:
$F(m) = m$

PKE	**IBE**	**ABE**
[DH76]	[S84]	[SW05]
[RSA77]	[BF01]	[GVW13]
[GM82]	[C01]	…

Identity-Based Encryption:

$$F_{ID}(x, m) = \begin{cases} m & \text{if } x = ID \\ \perp & \text{otherwise} \end{cases}$$

Attribute-Based Encryption

$$\xrightarrow{\mathrm{Enc}(\phi, m)}$$

Alice

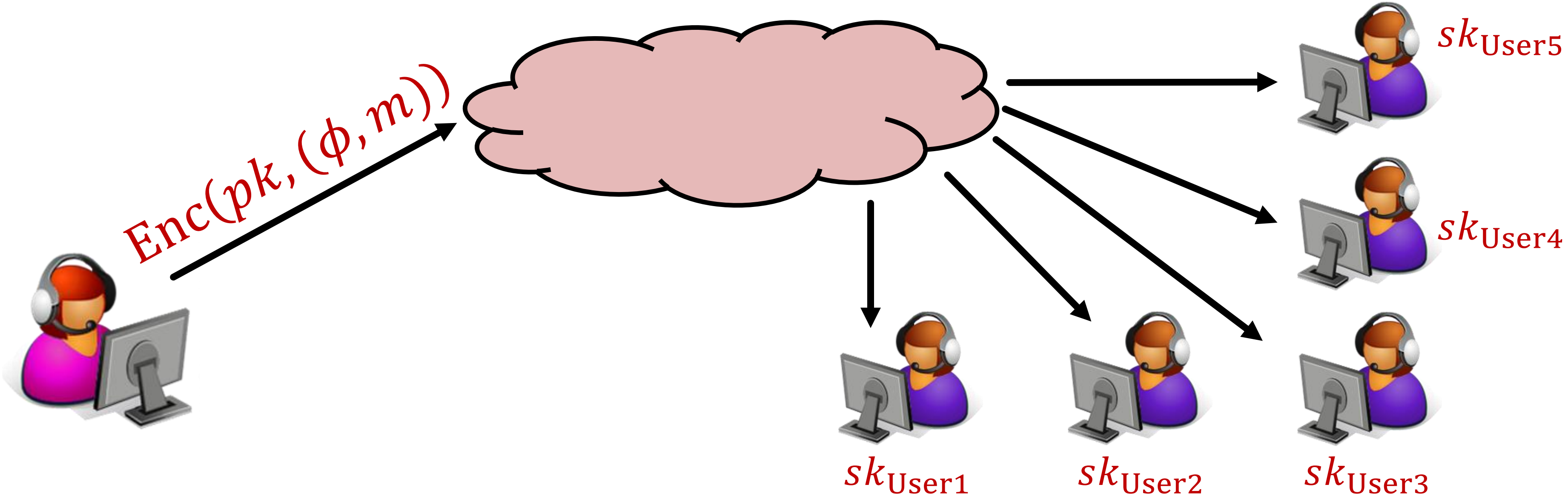
Access policy ϕ

Bob

Attribute-specific key sk_x

$$F_x(\phi, m) = \begin{cases} m & \text{if } \phi(x) = 1 \\ \perp & \text{otherwise} \end{cases}$$

Expressive Access Control



$$\phi = \left(\begin{pmatrix}\text{CEO's}\\ \text{Office}\end{pmatrix} \vee \begin{pmatrix}\text{Marketing \&}\\ \text{Location} = \text{CA}\end{pmatrix}\right) \bigwedge (\text{Age} \geq 24)$$

Attribute-Based Encryption

$\xrightarrow{\mathrm{Enc}(\phi, m)}$

Alice

Access policy ϕ

Bob

Attribute-specific key sk_x

Current status:

- Various schemes for specific predicates: Inner-product, subspace membership,…
- Recently: Schemes for all predicates based on lattices [GVW13,BGGHNSVV14] or multilinear maps [GGHSW13,GGHZ14]
- Extensive on-going research

The Road So Far

Public-Key Encryption:
$F(m) = m$

Attribute-Based Encryption:
$$F_\phi(x, m) = \begin{cases} m & \text{if } \phi(x) = 1 \\ \perp & \text{otherwise} \end{cases}$$

PKE **IBE** **ABE** **FE**

PKE	IBE	ABE	FE
[DH76]	[S84]	[SW05]	[GVW12,GKPVZ13]
[RSA77]	[BF01]	[GVW13]	[GHRSW13,W14]
[GM82]	[C01]	…	…

Identity-Based Encryption:
$$F_{ID}(x, m) = \begin{cases} m & \text{if } x = ID \\ \perp & \text{otherwise} \end{cases}$$

Functional Encryption:
Any function family!

Functional Encryption

Alice

Public key pk

Bob

Secret key sk_F

Learns $F(m)$
but nothing else
about m

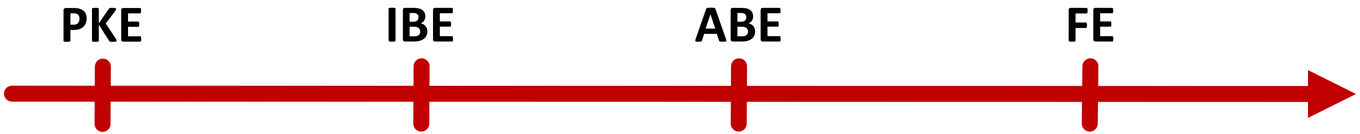
Current status:

- Bounded collusions with “long” ciphertexts based on any PKE [GVW12]
- Bounded collusions with “short” ciphertexts based on lattices [GKPVZ13]
- Unbounded collusions based on breakthroughs in program obfuscation [GHRSW13,W14]

The Road So Far

PKE	IBE	ABE	FE
[DH76]	[S84]	[SW05]	[GVW12,GKPVZ13]
[RSA77]	[BF01]	[GVW13]	[GHRSW13,W14]
[GM82]	[C01]	…	…

The Road So Far



[BF01]

Next:
The Boneh-Franklin IBE

The Boneh-Franklin IBE

(In fact, a simplified variant based on a stronger assumption)

Pairing-based cryptography:

- Let $\mathbb{G}$ and $\mathbb{G}_T$ be cyclic groups of prime order q
- Let $g \in \mathbb{G}$ be a generator of $\mathbb{G}$
- Let $e: \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ be a non-degenerate bilinear map:
  - $e(g, g)$ generates $\mathbb{G}_T$
  - $e(g^a, g^b) = e(g, g)^{ab}$ for all $a, b \in \mathbb{Z}_q$

Recall: ElGamal Encryption '84

Setup:
- Sample $sk = \alpha \leftarrow \mathbb{Z}_q$
- Let $pk = h = g^\alpha$

Encryption of $\boldsymbol{m}$:
- Sample $r \leftarrow \mathbb{Z}_q$
- Output $(c_0, c_1) = (g^r, h^r \cdot m)$

Decrypting (c_0, c_1) using sk:

$$\frac{c_1}{(c_0)^\alpha} = \frac{h^r \cdot m}{g^{r\alpha}} = \frac{g^{\alpha r} \cdot m}{g^{r\alpha}} = m$$

The Decisional Diffie-Hellman (DDH) Assumption:

$$(g, g^\alpha, g^r, g^{\alpha r}) \approx^c (g, g^\alpha, g^r, g^z)$$

where $\alpha, r, z \leftarrow \mathbb{Z}_q$.

Recall: ElGamal Encryption '84

Setup:
- Sample $sk = \alpha \leftarrow \mathbb{Z}_q$
- Let $pk = h = g^\alpha$

Encryption of m:
- Sample $r \leftarrow \mathbb{Z}_q$
- Output $(c_0, c_1) = (g^r, h^r \cdot m)$

Boneh-Franklin '01: From ElGamal to IBE
- For each ID implicitly define pk_{ID} by "projecting" pk onto ID in $\mathbb{G}_T$
- Encrypt to pk_{ID} by splitting El-Gamal between $\mathbb{G}$ and $\mathbb{G}_T$
- Security proof: Projections are "computationally independent"

$$pk = h \xrightarrow{ID} pk_{ID} = e\big(h, H(ID)\big)$$

$$sk = \alpha \xrightarrow{ID} sk_{ID} = H(ID)^\alpha$$

The Boneh-Franklin IBE

Setup:
- Sample $sk = \alpha \leftarrow \mathbb{Z}_q$
- Let $pk = h = g^\alpha$

Key generation for $\boldsymbol{ID}$:
- Output $sk_{ID} = H(ID)^\alpha$

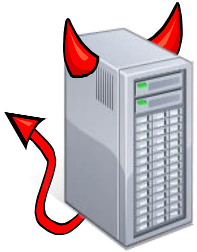
Encryption of $(\boldsymbol{ID}, \boldsymbol{m})$:
- Sample $r \leftarrow \mathbb{Z}_q$ and output $(c_0, c_1) = \left(g^r, e\big(h, H(ID)\big)^r \cdot m\right)$

Decrypting (c_0, c_1) using sk_{ID}:

$$\frac{c_1}{e(c_0, sk_{ID})} = \frac{e\big(h, H(ID)\big)^r \cdot m}{e(g^r, H(ID)^\alpha)} = \frac{e\big(g^\alpha, H(ID)\big)^r \cdot m}{e(g^r, H(ID)^\alpha)} = m$$

IBE Security

Public key
pk



Output a
guess b'

ID

sk_{ID}

$ID^*, (m_0, m_1)$

$\mathrm{Enc}\big(pk, (ID^*, m_b)\big)$

ID

sk_{ID}

Secret key
sk

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

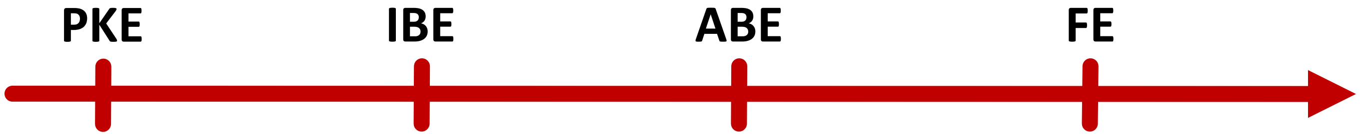
IBE security requirement:
For any efficient adversary $|\Pr[b' = b] - 1/2|$ is negligible

This Talk

- **Direct applications**
- **The security of functional encryption**
- **The road so far: From public-key to functional encryption**
- **The road ahead**

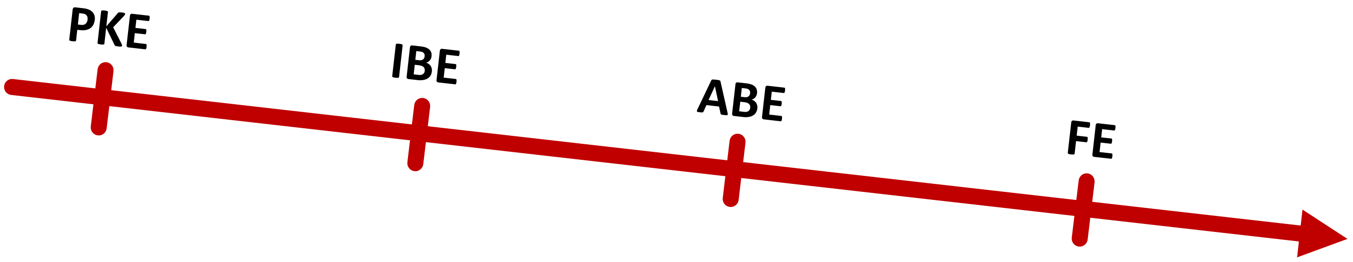
The Road Ahead

- **We are current losing the functionality vs. efficiency battle**
  - Deployment beyond identity-based encryption?
  - Better efficiency in the symmetric-key setting?



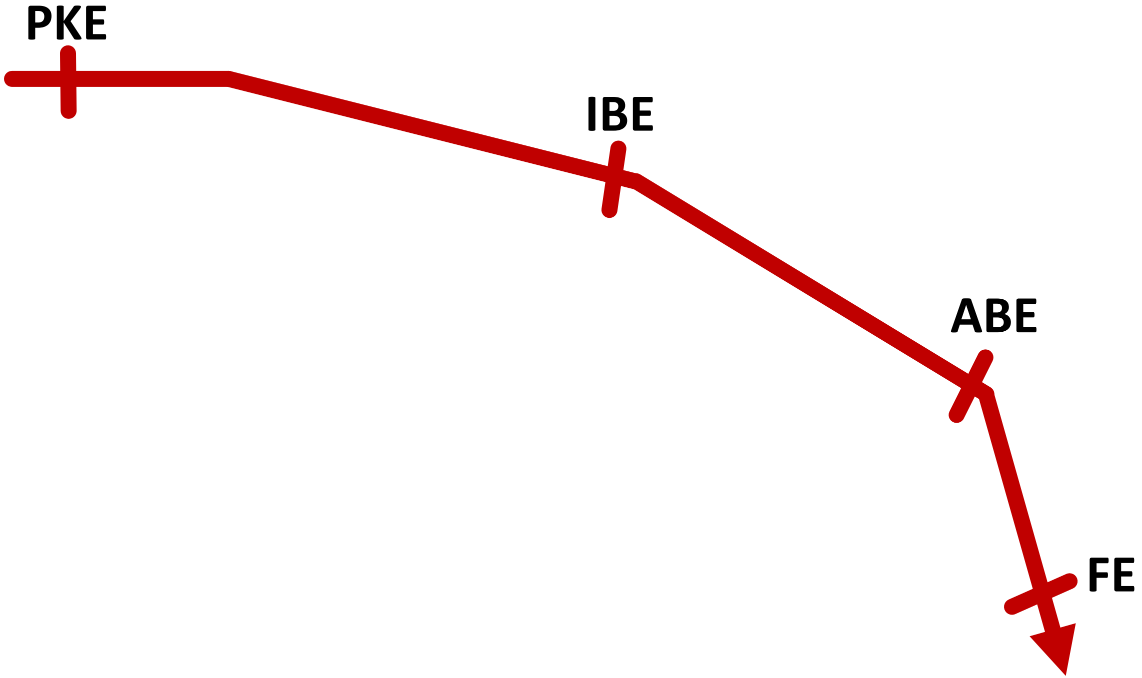
The Road Ahead

- **We are current losing the functionality vs. efficiency battle**
  - Deployment beyond identity-based encryption?
  - Better efficiency in the symmetric-key setting?



The Road Ahead

- **We are current losing the functionality vs. efficiency battle**
  - Deployment beyond identity-based encryption?
  - Better efficiency in the symmetric-key setting?



The Road Ahead

- **We are current losing the functionality vs. efficiency battle**
  - Deployment beyond identity-based encryption?
  - Better efficiency in the symmetric-key setting?
- **More schemes based on more standard assumptions**
  - More bilinear maps & lattices
  - Less obfuscation
  - Weaker assumptions in the symmetric-key setting? [ABSV14,BS15,KSY15]
- **Better security for functional encryption**
  - Function privacy: Does sk_F reveal F? [BRS13,…]
  - Application-specific security (e.g., deduplication [BKR13,ABMRS13,…])
- **We're just getting started…**

Thank You

www.cs.huji.ac.il/~segev