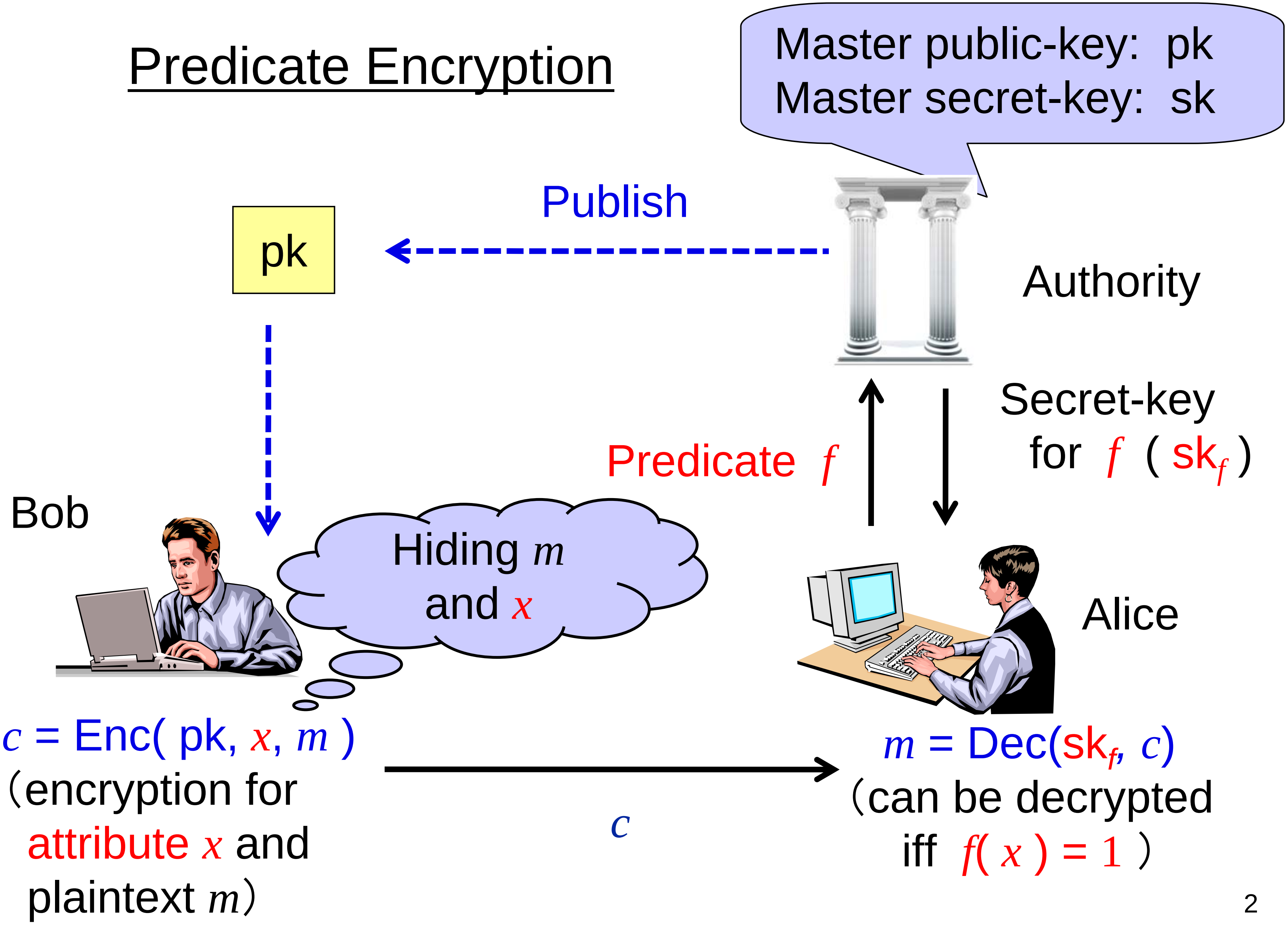
Adaptively Attribute-Hiding (Hierarchical) Inner Product Encryption

2011 / 8 / 16

Tatsuaki Okamoto (NTT),
Katsuyuki Takashima (Mitsubishi Electric).

Predicate Encryption



Master public-key: pk
Master secret-key: sk

Publish

pk

Authority

Predicate f

Secret-key for f (sk_f)

Bob

Hiding m and x

Alice

c = Enc(pk, x, m)
（encryption for attribute x and plaintext m）

c

m = Dec(sk_f, c)
（can be decrypted iff $f(x) = 1$ ）

Inner Product Encryption (IPE) [KSW08]

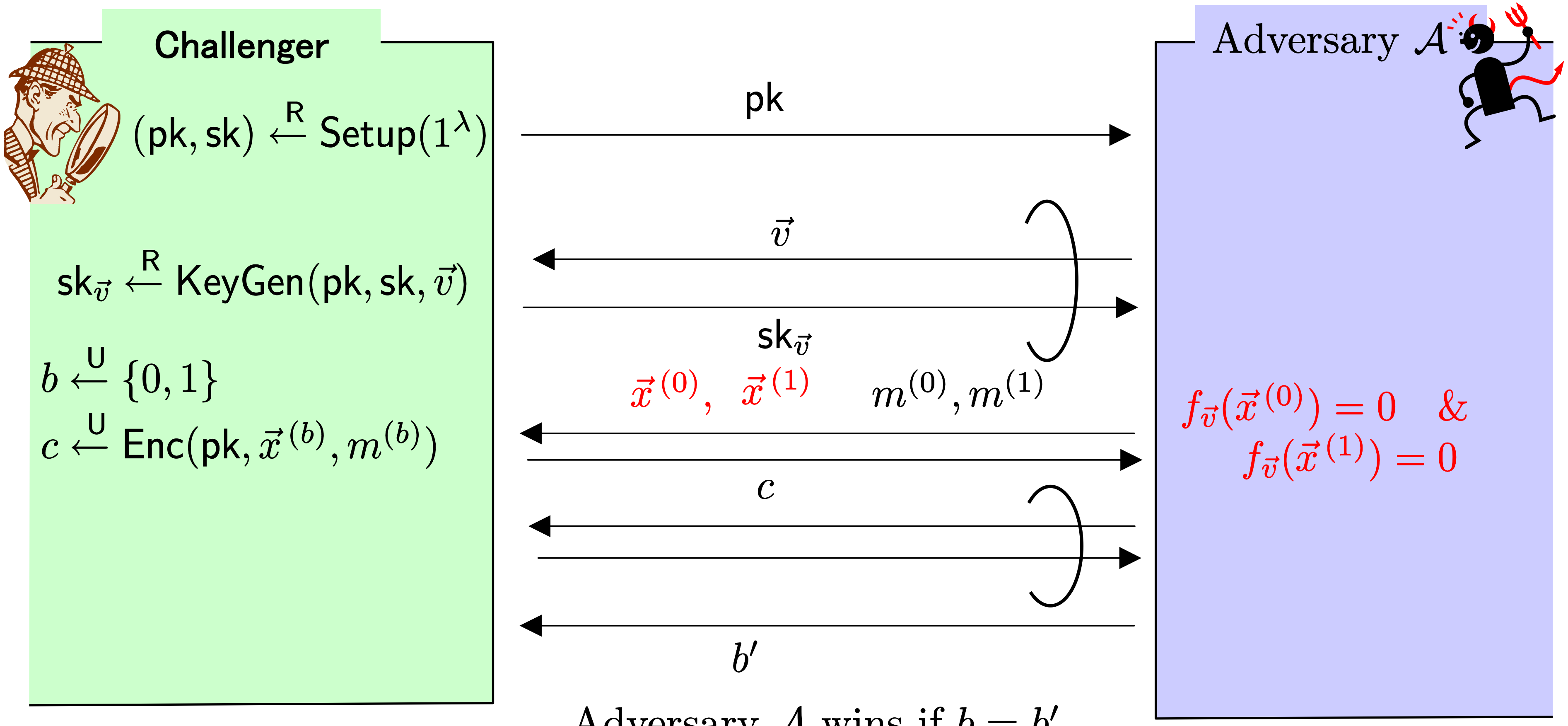
- $f_{\vec{v}}(\vec{x}) = 1$ iff $\vec{x} \cdot \vec{v} = 0$

  $f_{\vec{v}}$: predicate with $\vec{v} \in \mathbb{F}_q^n$, $\vec{x} \in \mathbb{F}_q^n$: attribute

- Setup: pk: (master) public key, sk: (master) secret key
- $\mathsf{KeyGen}(\,\mathsf{pk}, \mathsf{sk}, \vec{v}\,)$: $\mathsf{sk}_{\vec{v}}$: secret key for $\vec{v}$
- $\mathsf{Enc}(\,\mathsf{pk}, \vec{x}, m\,)$: $c_{\vec{x}}$: ciphertext for $\vec{x}$
- $\mathsf{Dec}(\,\mathsf{pk}, \mathsf{sk}_{\vec{v}}, c\,)$: plaintext m or $\perp$

  m can be decrypted iff $f_{\vec{v}}(\vec{x}) = 1$, i.e., $\vec{x} \cdot \vec{v} = 0$

Weakly Attribute-Hiding Security of IPE



Challenger

$(\mathsf{pk},\mathsf{sk}) \overset{\mathsf{R}}{\longleftarrow} \mathsf{Setup}(1^\lambda)$

$\mathsf{sk}_{\vec{v}} \overset{\mathsf{R}}{\longleftarrow} \mathsf{KeyGen}(\mathsf{pk},\mathsf{sk},\vec{v})$

$b \overset{\mathsf{U}}{\longleftarrow} \{0,1\}$

$c \overset{\mathsf{U}}{\longleftarrow} \mathsf{Enc}(\mathsf{pk},\vec{x}^{\,(b)},m^{(b)})$

Adversary $\mathcal{A}$

pk

$\vec{v}$

$\mathsf{sk}_{\vec{v}}$

$\vec{x}^{\,(0)}, \quad \vec{x}^{\,(1)} \qquad m^{(0)}, m^{(1)}$

c

b'

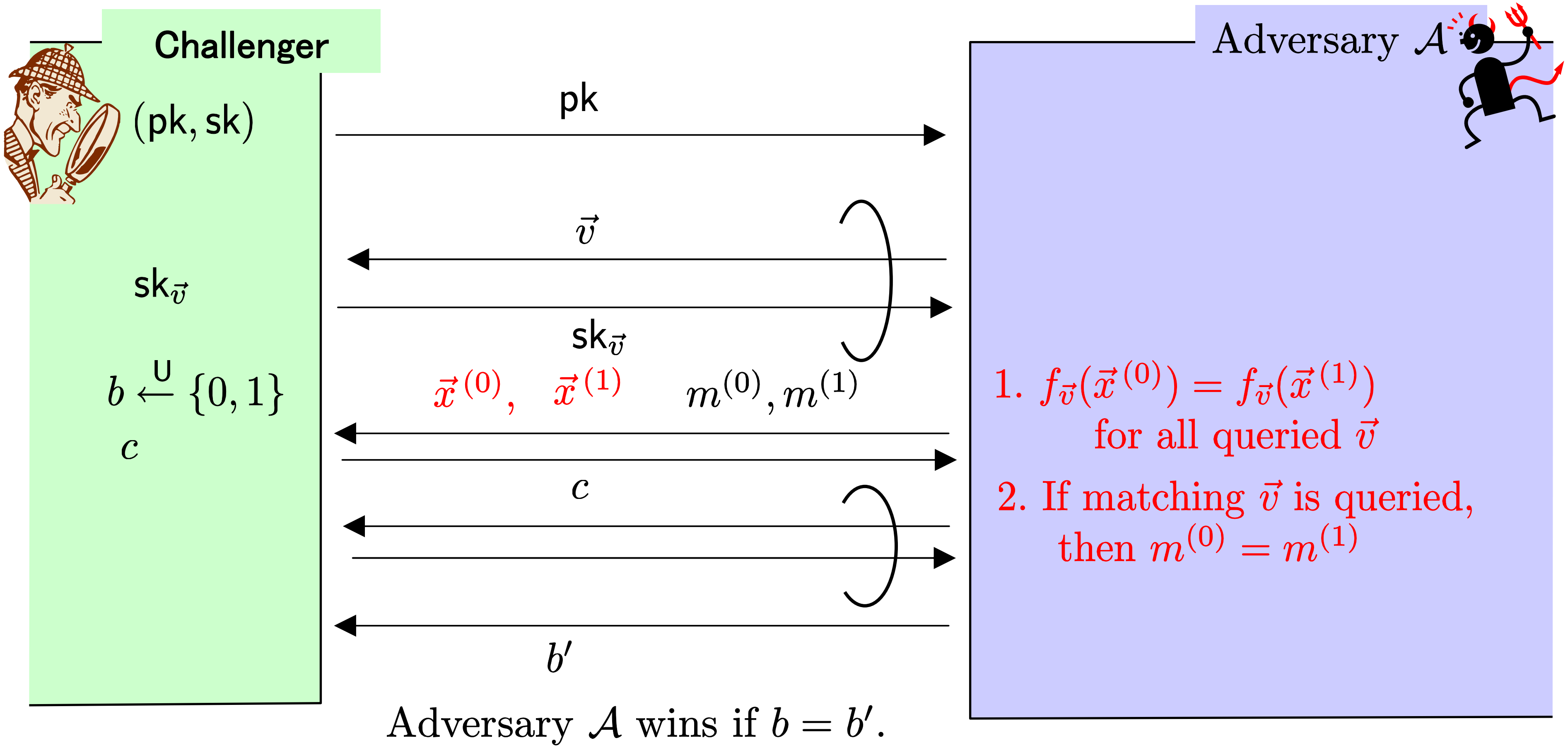
$f_{\vec{v}}(\vec{x}^{\,(0)}) = 0 \quad \&$

$f_{\vec{v}}(\vec{x}^{\,(1)}) = 0$

Adversary $\mathcal{A}$ wins if $b = b'$.

Some additional information on $\vec{x}$ may be revealed
to a person with a matching key $\mathsf{sk}_{\vec{v}}$, i.e., $f_{\vec{v}}(\vec{x}) = 1$.

Fully Attribute-Hiding Security of IPE



Challenger

$(\mathsf{pk}, \mathsf{sk})$

$\mathsf{sk}_{\vec{v}}$

$b \overset{\mathsf{U}}{\leftarrow} \{0,1\}$

c

pk

$\vec{v}$

$\mathsf{sk}_{\vec{v}}$

$\vec{x}^{\,(0)}, \quad \vec{x}^{\,(1)} \qquad m^{(0)}, m^{(1)}$

c

b'

Adversary $\mathcal{A}$

1. $f_{\vec{v}}(\vec{x}^{\,(0)}) = f_{\vec{v}}(\vec{x}^{\,(1)})$
   for all queried $\vec{v}$
2. If matching $\vec{v}$ is queried,
   then $m^{(0)} = m^{(1)}$

Adversary $\mathcal{A}$ wins if $b = b'$.

No additional information on $\vec{x}$ is revealed

even to any person with a matching key $\mathsf{sk}_{\vec{v}}$, i.e., $f_{\vec{v}}(\vec{x}) = 1$.

Previous works for (Pairing-Based) IPE

- [KSW08] : Fully attribute–hiding but selectively secure IPE
- [LOSTW10] : Adaptively secure but weakly attribute–hiding IPE based on a non–standard assumption
- [OT10] : Adaptively secure but weakly attribute–hiding IPE based on the DLIN assumption

Our result

- Adaptively secure and fully attribute–hiding IPE based on the DLIN assumption

Thank You !