Fully-Anonymous
Functional Proxy-Re-Encryption

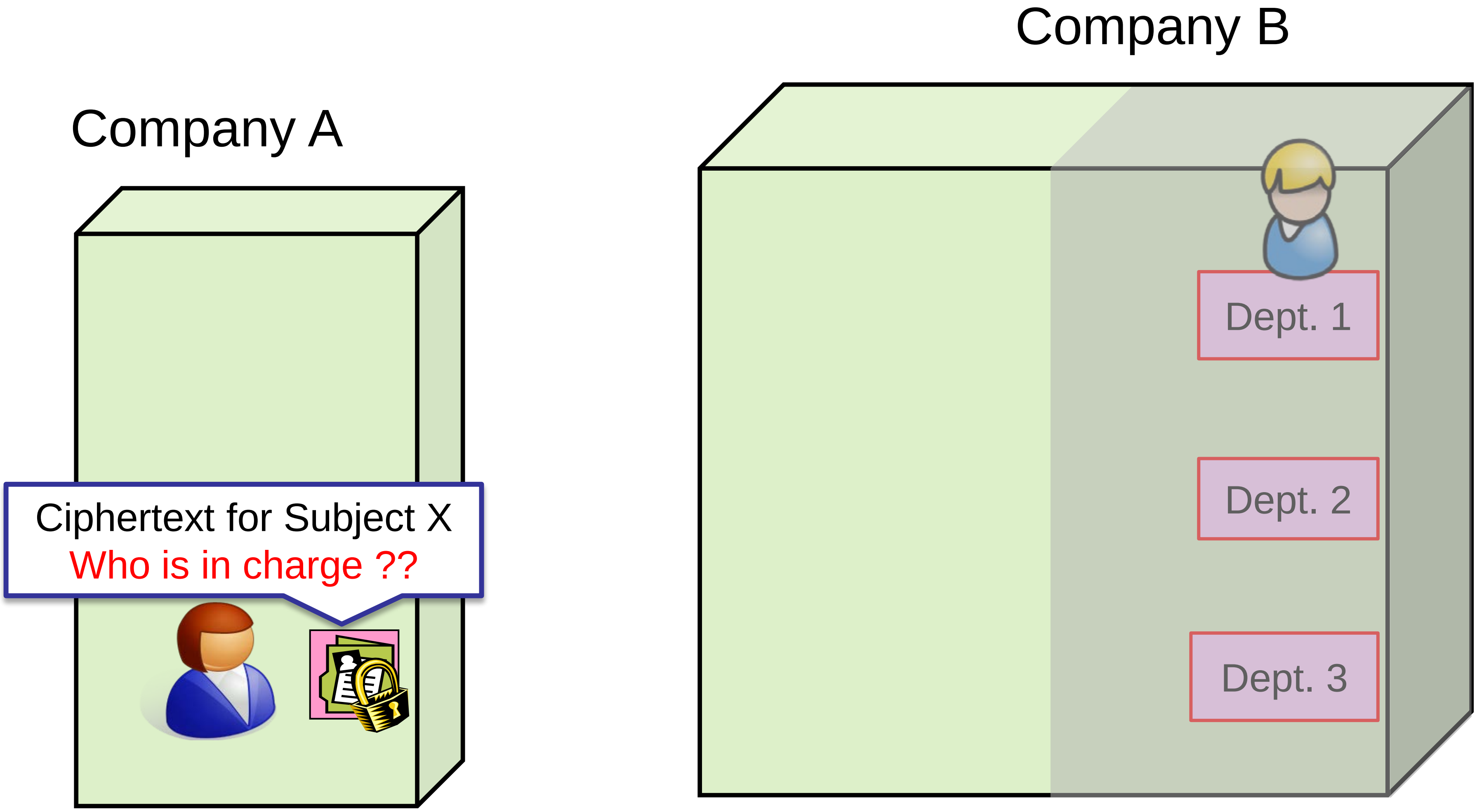
2013 / 8 / 20

Yutaka Kawai, Katsuyuki Takashima
(Mitsubishi Electric)

Available at http://eprint.iacr.org/2013/318

Motivation

Private communication among organizations with unknown or changeable inner structures



Company B

Company A

Dept. 1

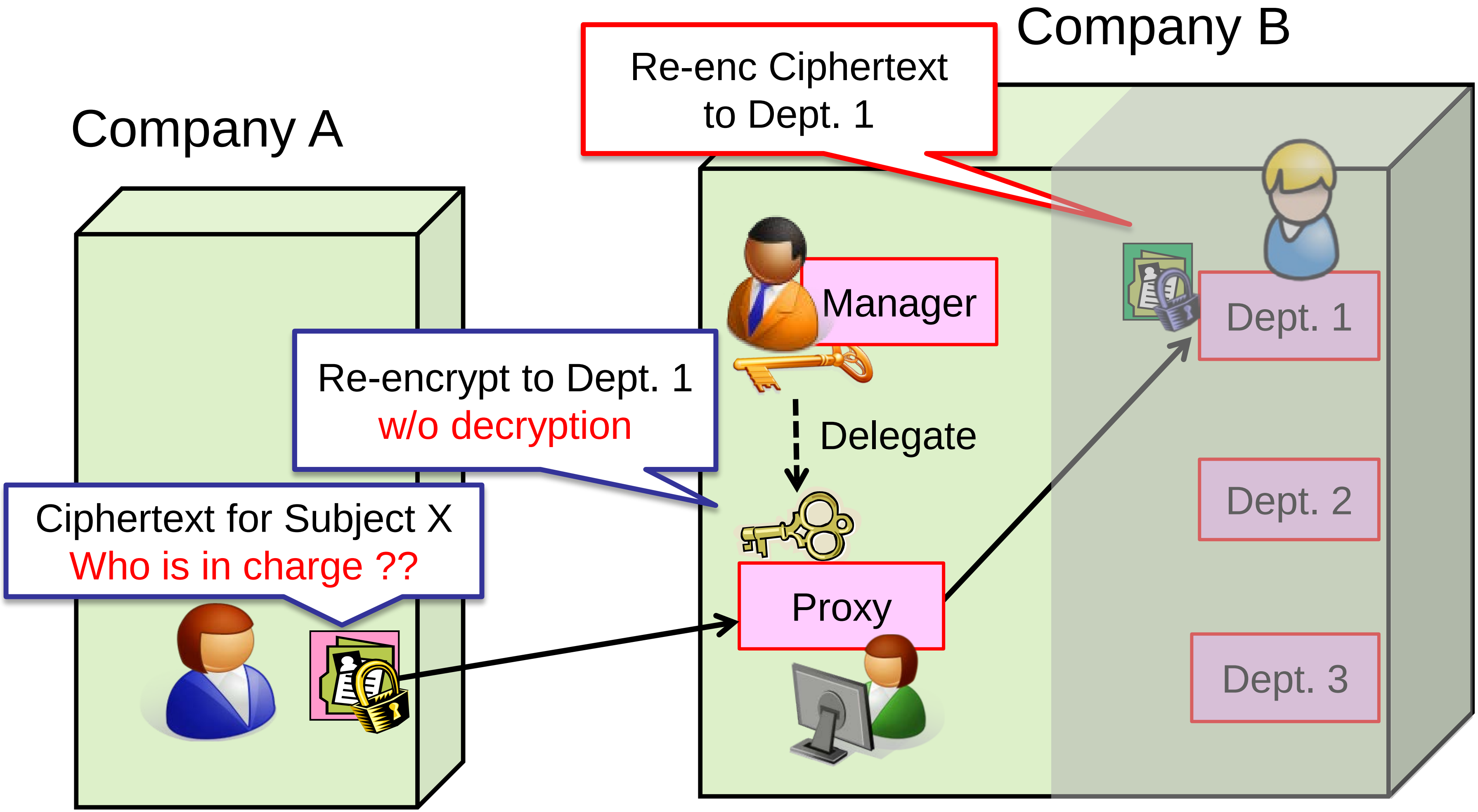
Dept. 2

Dept. 3

Ciphertext for Subject X
Who is in charge ??

Motivation

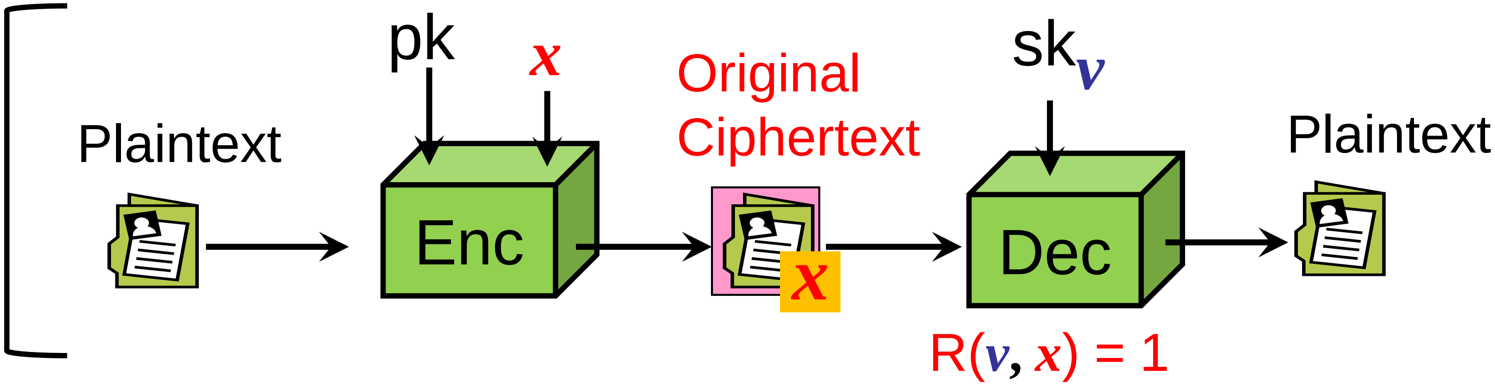
Private communication among organizations with unknown or changeable inner structures



Anonymous Attribute-Based Proxy-Re-Encryption

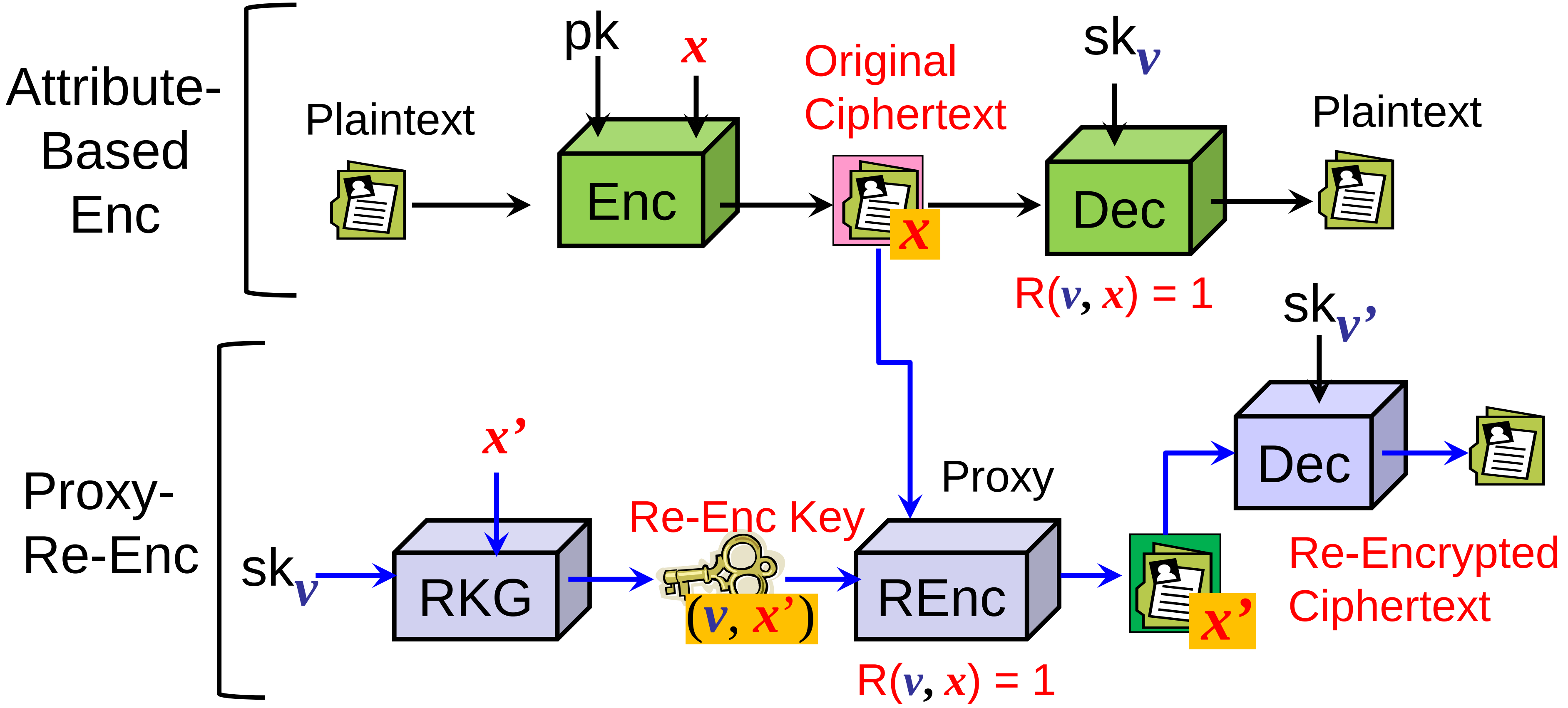
We use Attribute-Based Encryption with Anonymous Re-Encryption Functionality

Attribute-Based Enc



Anonymous Attribute-Based Proxy-Re-Encryption

We use Attribute-Based Encryption with
Anonymous Re-Encryption Functionality



Attribute-Based Enc

Plaintext

pk

x

Enc

Original Ciphertext

x

sk$_v$

Dec

Plaintext

$R(v, x) = 1$

sk$_{v'}$

Proxy-Re-Enc

sk$_v$

x'

RKG

Re-Enc Key

(v, x')

Proxy

REnc

$R(v, x) = 1$

x'

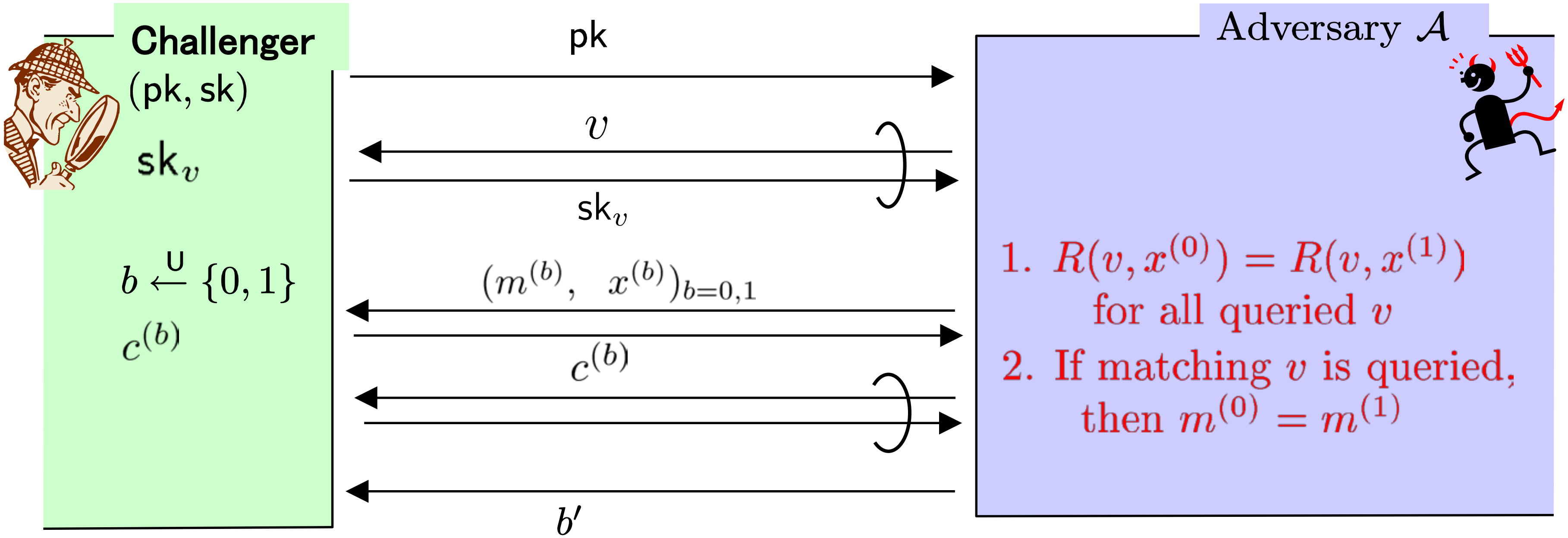
Dec

Re-Encrypted Ciphertext

Re-Encryption from parameter x to x' if $R(v, x) = 1$

Reminder: Fully Attribute-Hiding Inner Product Enc (IPE)

For $v, x \in \mathbb{F}_q^n$, $R(v,x) = 1$ iff $v \cdot x = 0$



Challenger

(pk, sk)

sk_v

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

$c^{(b)}$

pk

v

sk_v

$(m^{(b)}, \quad x^{(b)})_{b=0,1}$

$c^{(b)}$

b'

Adversary $\mathcal{A}$

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

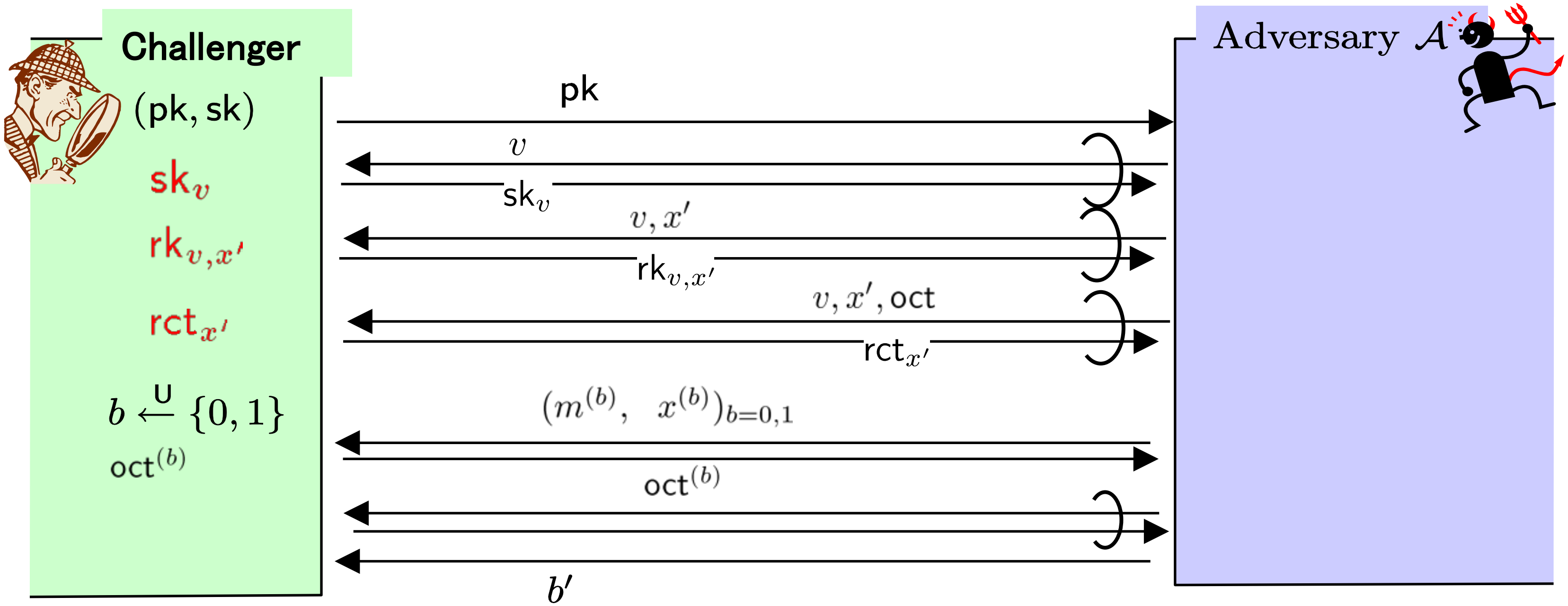
Adversary $\mathcal{A}$ wins if $b = b'$.

Ciphertext (CT) Indistinguishability under condition

$m^{(0)} \bullet R(v, x^{(0)}) = m^{(1)} \bullet R(v, x^{(1)})$ for any dec. key query v

where $X \bullet R(v,x) =$ " X if $R(v,x) = 1$, $\perp$ if $R(v,x) = 0$ "

Fully Attribute-Hiding for Original CT



Challenger

(pk, sk)

sk_v

$\mathsf{rk}_{v,x'}$

$\mathsf{rct}_{x'}$

$b \xleftarrow{\mathsf{U}} \{0,1\}$

$\mathsf{oct}^{(b)}$

Adversary $\mathcal{A}$

pk

v

sk_v

v, x'

$\mathsf{rk}_{v,x'}$

v, x', oct

$\mathsf{rct}_{x'}$

$(m^{(b)}, x^{(b)})_{b=0,1}$

$\mathsf{oct}^{(b)}$

b'

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

Original CT Indistinguishability under

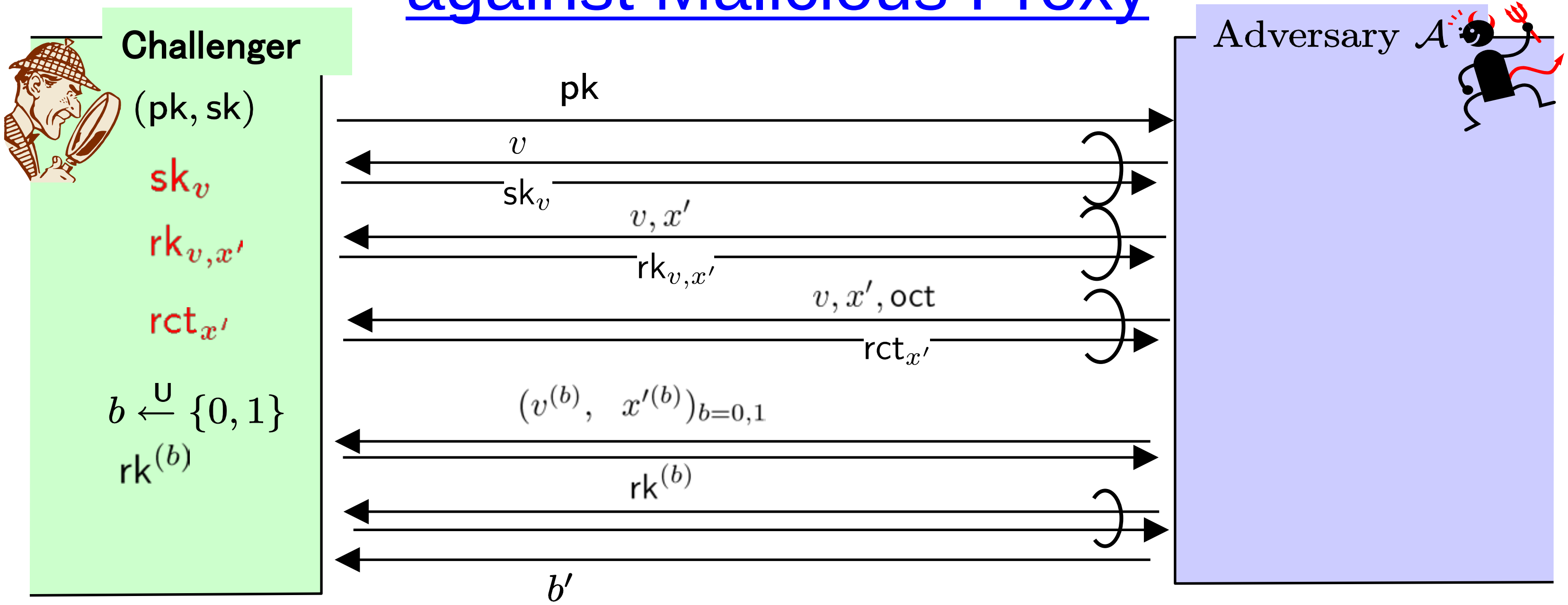
$$m^{(0)} \bullet R(v, x^{(0)}) = m^{(1)} \bullet R(v, x^{(1)})$$

$$m^{(0)} \bullet R(v_\ell, x^{(0)}) \bullet R(v, x'_\ell) = m^{(1)} \bullet R(v, x^{(1)}) \bullet R(v, x'_\ell)$$

for any dec. key query v and re-enc. key query (v_ℓ, x'_ℓ)

Security against re-enc. attack for original CT

Predicate- and Attribute-Hiding for Re-Encryption Key against Malicious Proxy



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

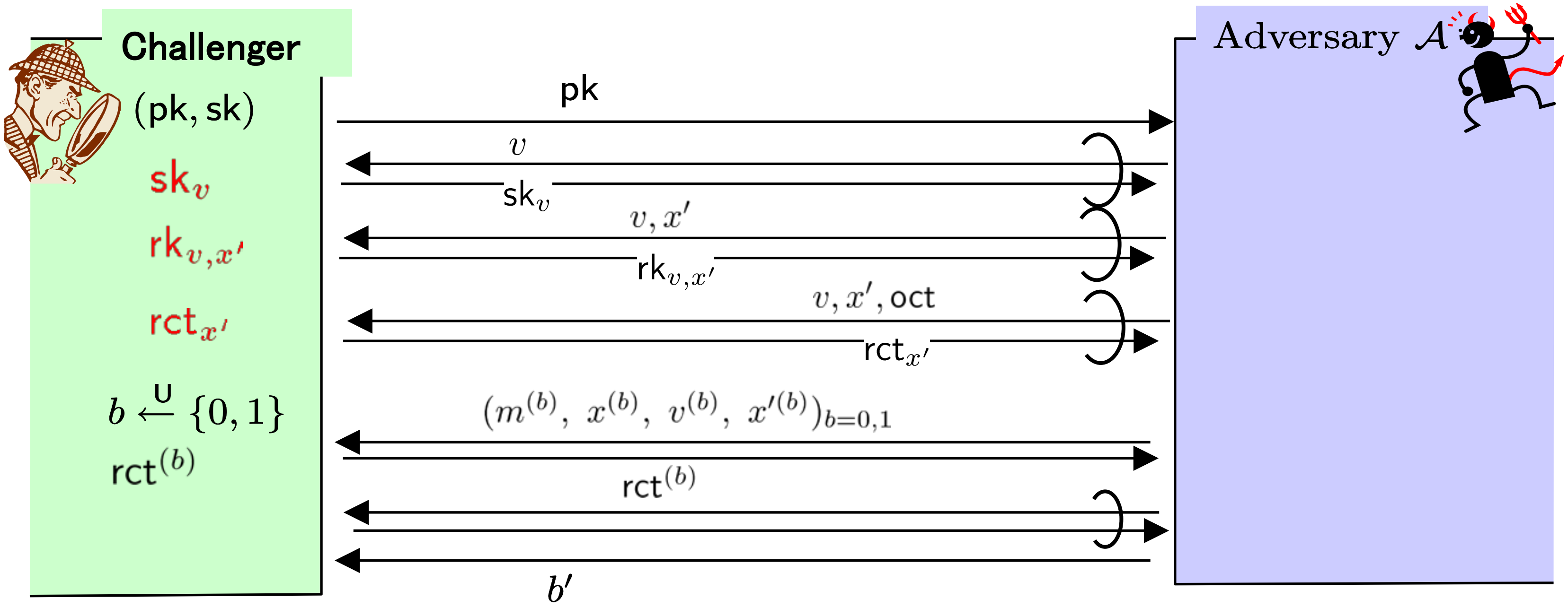
Re-Encryption Key Indistinguishability under condition

$$v^{(0)} \bullet R(v', x'^{(0)}) = v^{(1)} \bullet R(v', x'^{(1)})$$

for any dec. key query v'

Hiding $(v^{(b)}, \ x'^{(b)})$ against proxy

Predicate- and Attribute-Hiding for Re-Encrypted CT



Challenger

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

sk_v

$\mathsf{rk}_{v,x'}$

$\mathsf{rct}_{x'}$

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

$\mathsf{rct}^{(b)}$

Adversary $\mathcal{A}$

pk

v

sk_v

v, x'

$\mathsf{rk}_{v,x'}$

v, x', oct

$\mathsf{rct}_{x'}$

$(m^{(b)},\ x^{(b)},\ v^{(b)},\ x'^{(b)})_{b=0,1}$

$\mathsf{rct}^{(b)}$

b'

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

Re-Encrypted CT Indistinguishability under condition

$$(m^{(0)}, x^{(0)}, v^{(0)}) \bullet R(v', x'^{(0)}) = (m^{(1)}, x^{(1)}, v^{(1)}) \bullet R(v', x'^{(1)})$$

for any dec. key query v'

Full Anonymity

An AB-PRE (or functional-PRE) is fully-anonymous
if it satisfies the following requirements

1. Attribute-Hiding for Original CTs
2. Predicate- and Attribute-Hiding for Re-Encryption Keys
3. Predicate- and Attribute-Hiding for Re-Encrypted CTs

4. (Unconditional) Unlinkability of Re-Encryption Keys
5. (Computational) Unlinkability of Re-Encrypted CTs

Our Results

1. Introduction of a new notion of functional proxy-re-encryption (F-PRE) and full anonimity
2. The first fully-anonymous inner-product proxy-re-encryption (IP-PRE) scheme, whose security is proven under
    - the DLIN assumption and
    - the existence of a strongly unforgeable one-time signature scheme

    in the standard model.
3. The first ciphertext-policy (CP-) F-PRE scheme with the access structure class given by Okamoto-Takashima [OT10].

Key Techniques

Blind Delegation, New Hidden Subspace Generation,

Dual Pairing Vector Space (DPVS) Framework

Thank You !

Available at http://eprint.iacr.org/2013/318