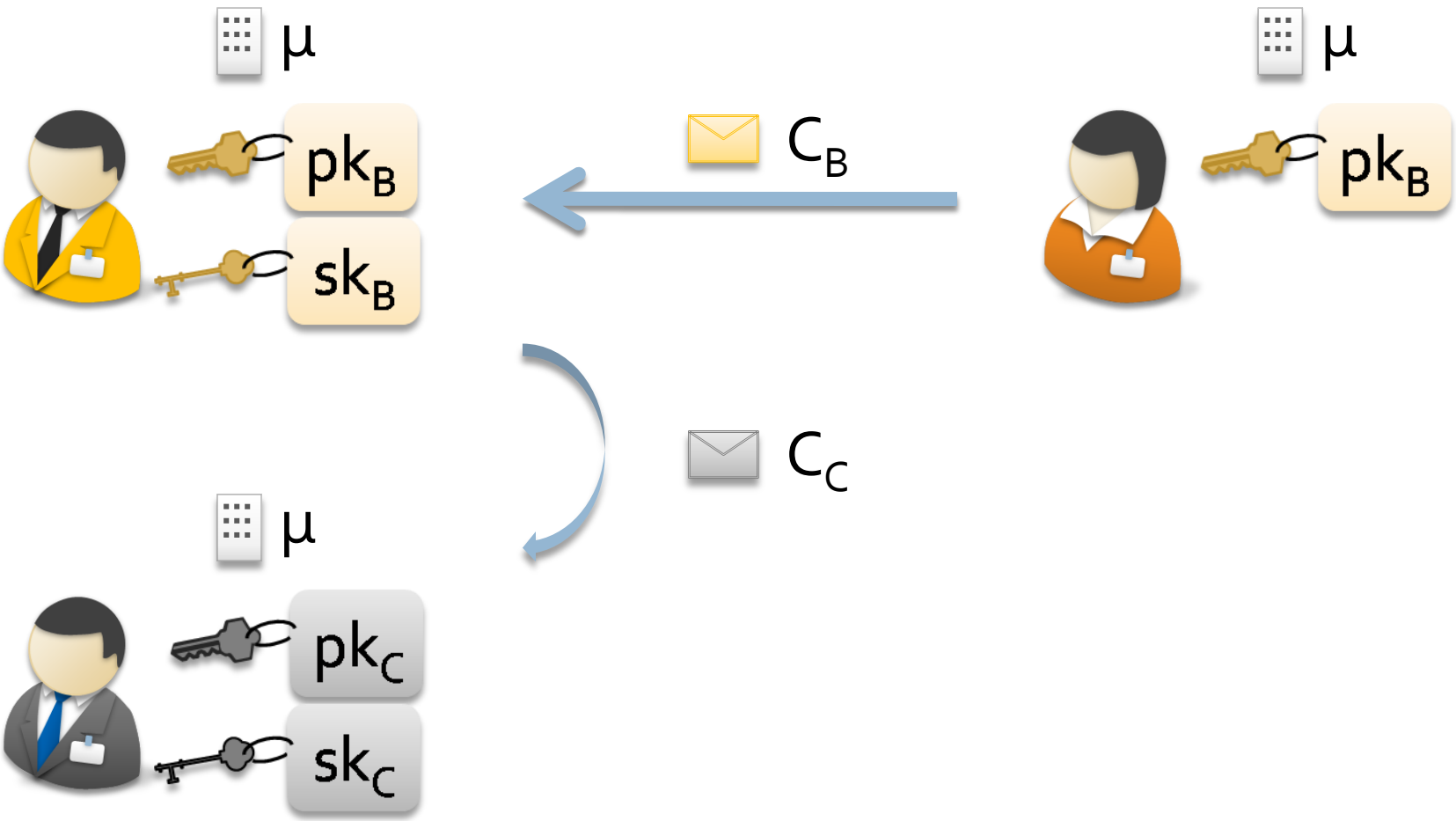
Proxy Re-Encryptions from Learning with Errors

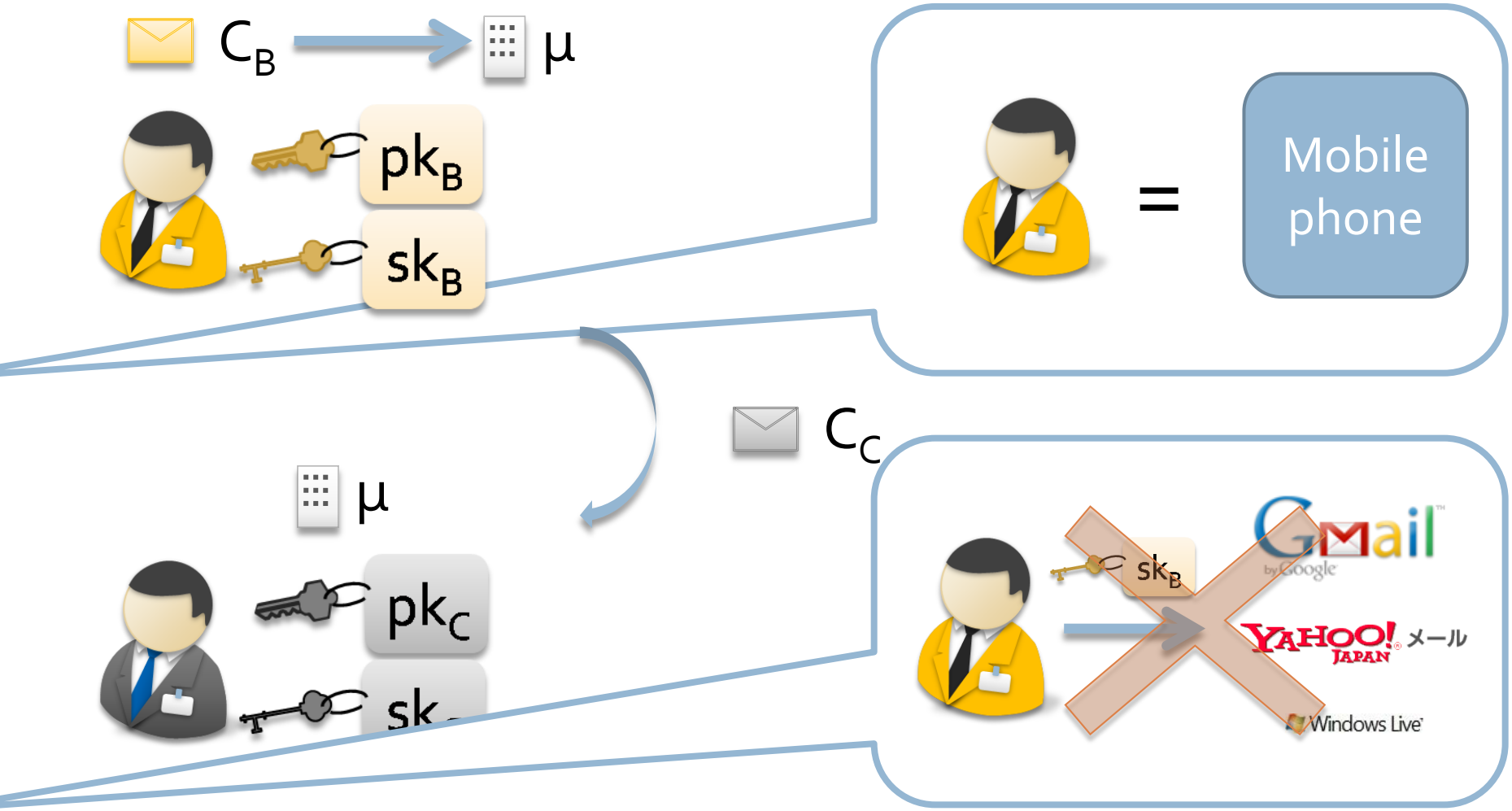
Keita Xagawa and Keisuke Tanaka

(Tokyo Institute of Technology)

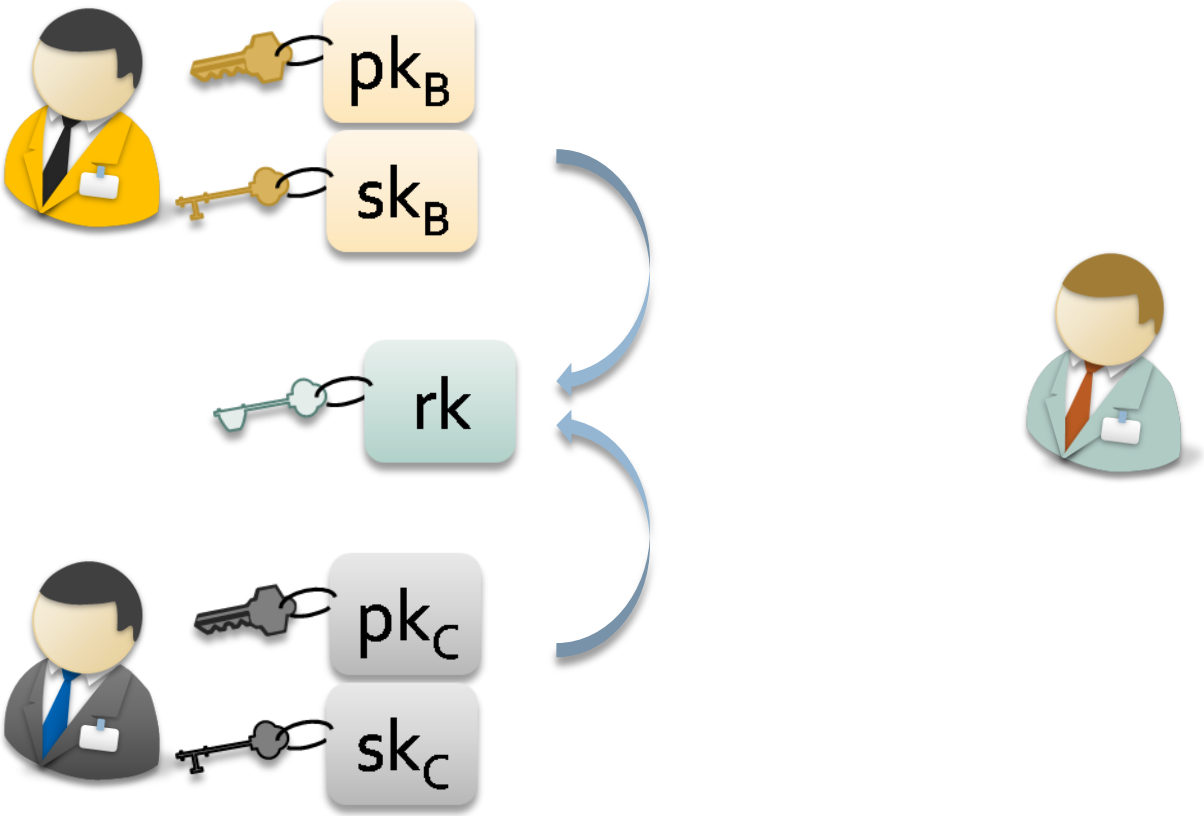
E-mail Forwarding



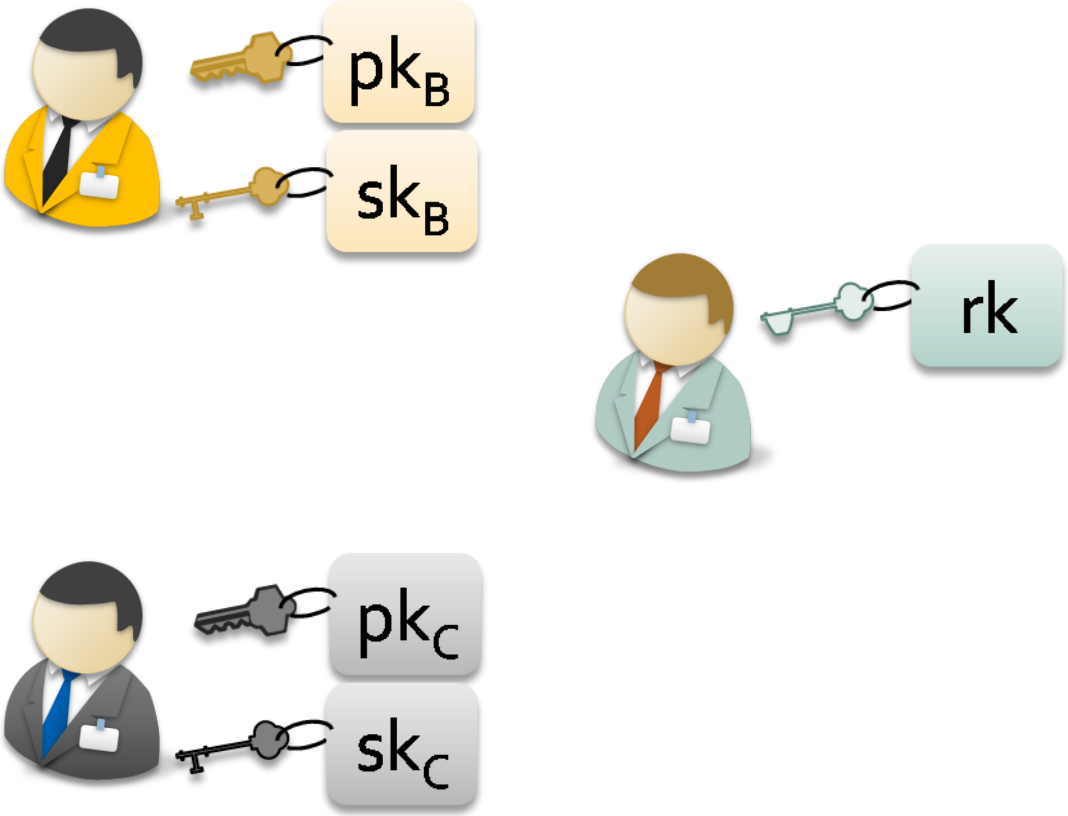
E-mail Forwarding



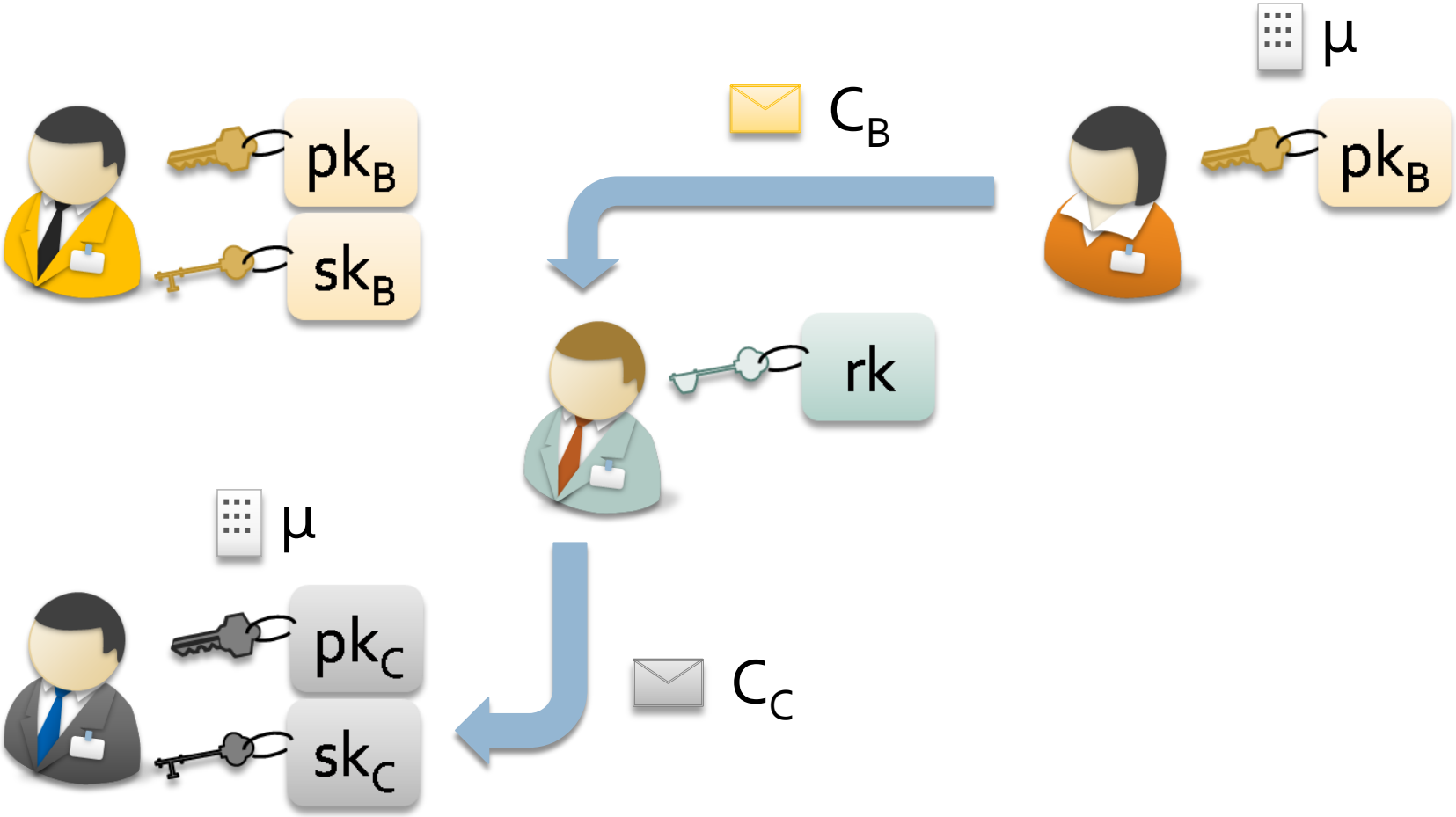
Proxy Re-Encryption (PRE)



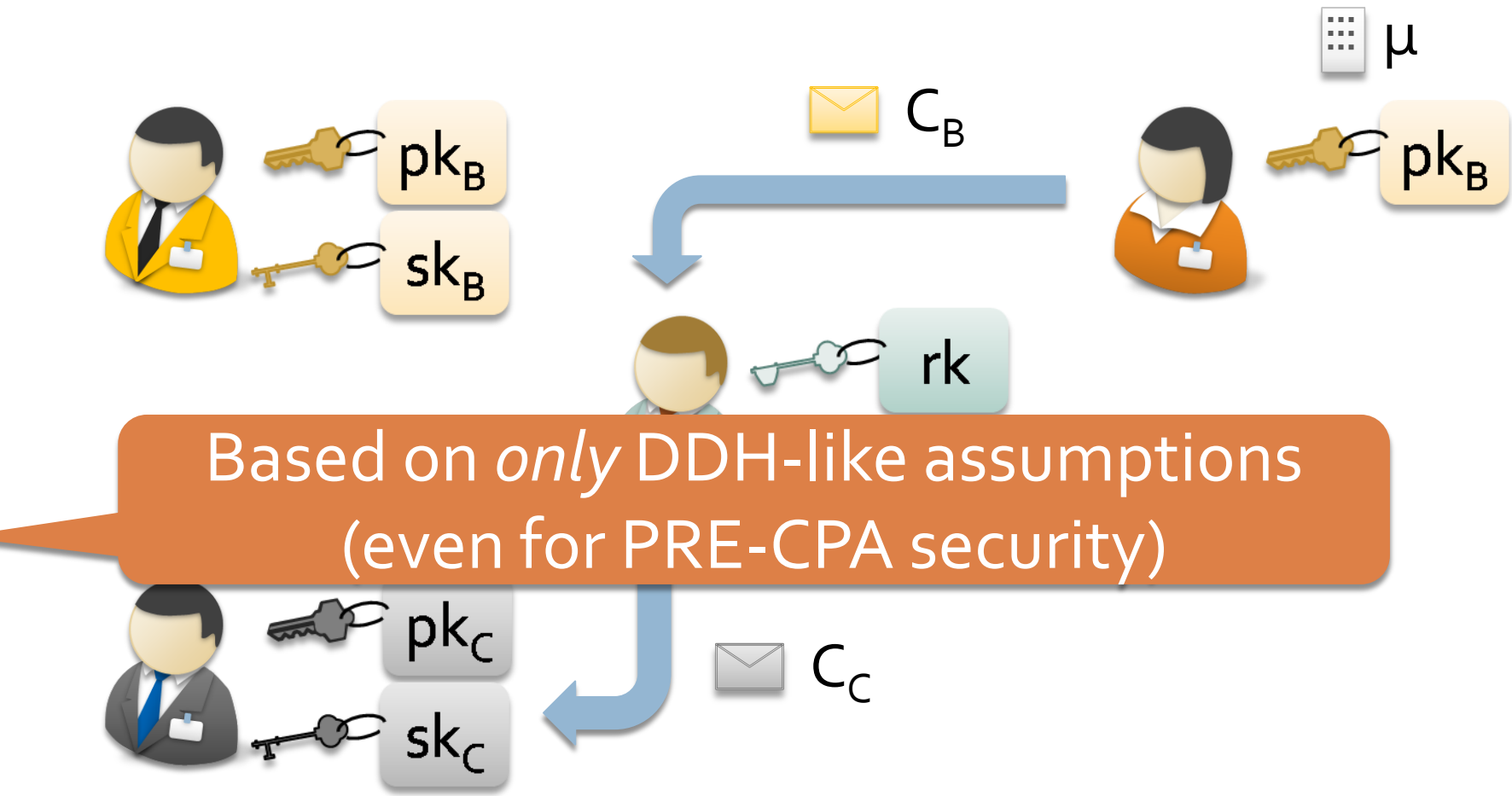
Proxy Re-Encryption (PRE)



Proxy Re-Encryption (PRE)



Proxy Re-Encryption (PRE)

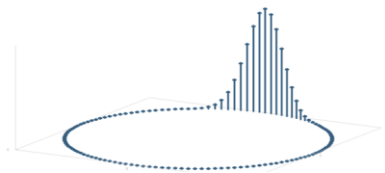


LWE assumption

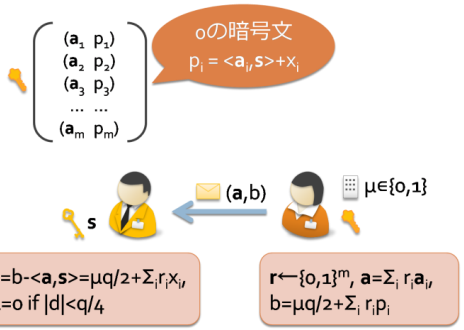
$A_{s,\chi}$
1. $\mathbf{a} \leftarrow \mathbb{Z}_q^n$, $x \leftarrow \chi$
2. $p = \langle \mathbf{a}, \mathbf{s} \rangle + x$
3. Output $(\mathbf{a}, p)$

$\equiv_c$

U
1. $\mathbf{a} \leftarrow \mathbb{Z}_q^n$,
2. $u \leftarrow \mathbb{Z}_q$
3. Output $(\mathbf{a}, u)$



PKE

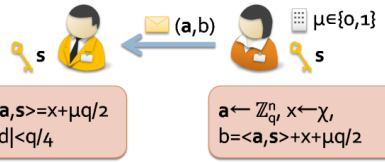


SKE

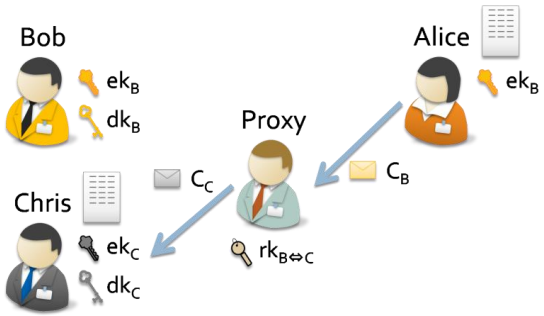
$A_{s,\chi}$
1. $\mathbf{a} \leftarrow \mathbb{Z}_q^n$, $x \leftarrow \chi$
2. $p = \langle \mathbf{a}, \mathbf{s} \rangle + x$
3. Output $(\mathbf{a}, p)$

$\equiv_c$

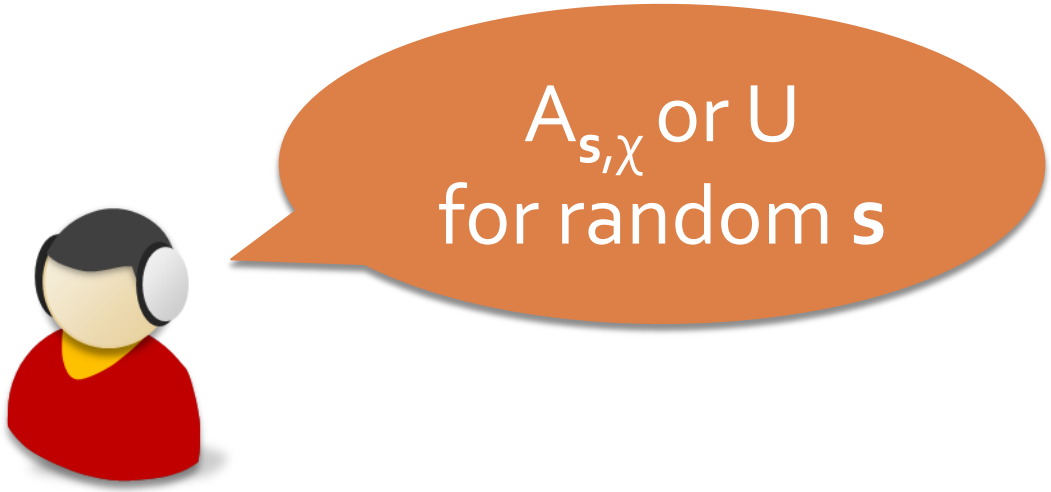
U
1. $\mathbf{a} \leftarrow \mathbb{Z}_q^n$,
2. $u \leftarrow \mathbb{Z}_q$
3. Output $(\mathbf{a}, u)$



PRE



$LWE_{q,\chi}$



$A_{s,\chi}$

1. $\mathbf{a} \leftarrow \mathbb{Z}_q^n$, $x \leftarrow \chi$
2. $p = \langle \mathbf{a}, \mathbf{s} \rangle + x$
3. Output $(\mathbf{a}, p)$

U

1. $\mathbf{a} \leftarrow \mathbb{Z}_q^n$,
2. $u \leftarrow \mathbb{Z}_q$
3. Output $(\mathbf{a}, u)$

$LWE_{q,\chi}$ Assumption

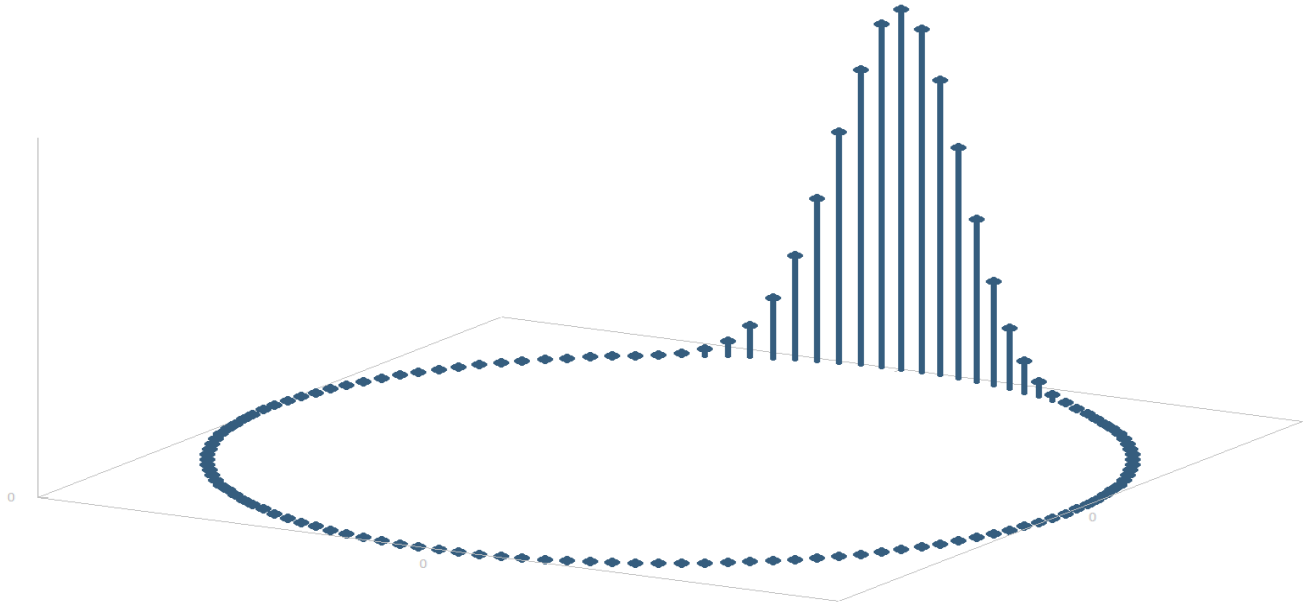
$A_{s,\chi}$

1. $\mathbf{a} \leftarrow \mathbb{Z}_q^n$, $x \leftarrow \chi$
2. $p = \langle \mathbf{a}, \mathbf{s} \rangle + x$
3. Output $(\mathbf{a}, p)$

$\equiv_c$

U

1. $\mathbf{a} \leftarrow \mathbb{Z}_q^n$,
2. $u \leftarrow \mathbb{Z}_q$
3. Output $(\mathbf{a}, u)$

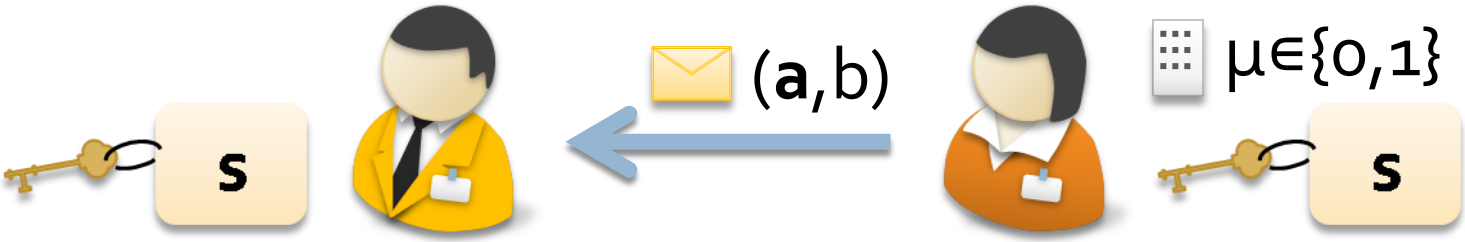


LWE-based SKE

$A_{s,\chi}$
1. $\mathbf{a} \leftarrow \mathbb{Z}_q^n$, $x \leftarrow \chi$
2. $p = \langle \mathbf{a}, \mathbf{s} \rangle + x$
3. Output $(\mathbf{a}, p)$

$\equiv_c$

U
1. $\mathbf{a} \leftarrow \mathbb{Z}_q^n$,
2. $u \leftarrow \mathbb{Z}_q$
3. Output $(\mathbf{a}, u)$



$d = b - \langle \mathbf{a}, \mathbf{s} \rangle = x + \mu q/2$
$\mu = 0$ if $|d| < q/4$

$\mathbf{a} \leftarrow \mathbb{Z}_q^n$, $x \leftarrow \chi$,
$b = \langle \mathbf{a}, \mathbf{s} \rangle + x + \mu q/2$

LWE-based SKE — linearity

$(\mathbf{a}_1, b_1) + (\mathbf{a}_2, b_2) \sim (\mathbf{a}_3, b_3)$

$\mu_1 + \mu_2 = \mu_1 + \mu_2$

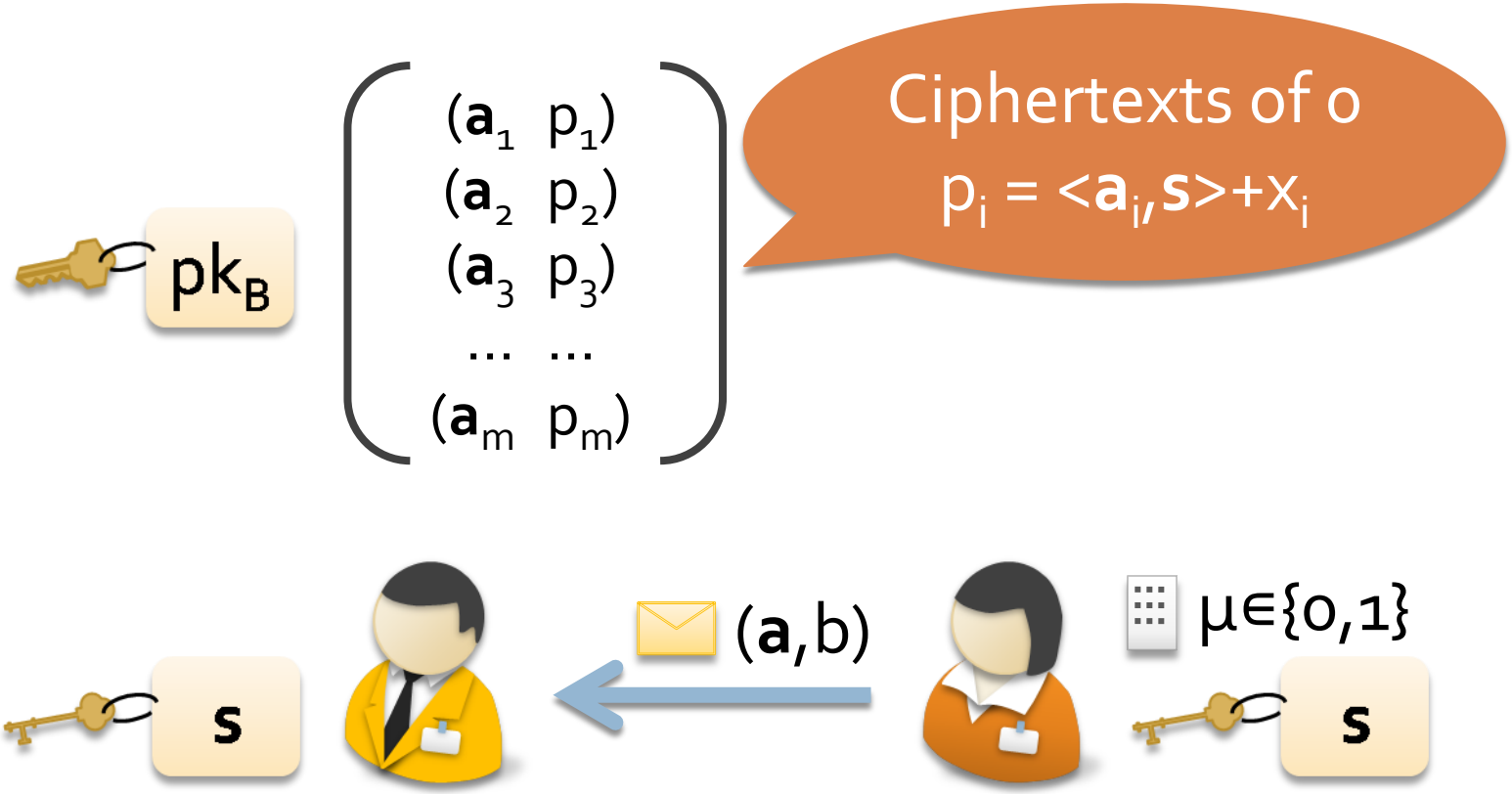
$(\mathbf{a}_1, b_1) = (\mathbf{a}_1, \langle \mathbf{a}_1, \mathbf{s} \rangle + x_1 + \mu_1 q/2)$
$(\mathbf{a}_2, b_2) = (\mathbf{a}_2, \langle \mathbf{a}_2, \mathbf{s} \rangle + x_2 + \mu_2 q/2)$

$(\mathbf{a}_3, b_3) = (\mathbf{a}_1 + \mathbf{a}_2, \langle \mathbf{a}_1 + \mathbf{a}_2, \mathbf{s} \rangle + x_1 + x_2 + (\mu_1 + \mu_2) q/2)$

$d = b - \langle \mathbf{a}, \mathbf{s} \rangle = x + \mu q/2$
$\mu = 0$ if $|d| < q/4$

$\mathbf{a} \leftarrow \mathbb{Z}_q^n$, $x \leftarrow \chi$,
$b = \langle \mathbf{a}, \mathbf{s} \rangle + x + \mu q/2$

LWE-based PKE



$d = b - \langle \mathbf{a}, \mathbf{s} \rangle = x + \mu q/2$

$\mu = 0$ if $|d| < q/4$

$\mathbf{a} \leftarrow \mathbb{Z}_q^n$, $x \leftarrow \chi$,

$b = \langle \mathbf{a}, \mathbf{s} \rangle + x + \mu q/2$

LWE-based PKE

pk_B

$$\begin{pmatrix} (\mathbf{a}_1 & p_1) \\ (\mathbf{a}_2 & p_2) \\ (\mathbf{a}_3 & p_3) \\ \dots & \dots \\ (\mathbf{a}_m & p_m) \end{pmatrix}$$

Ciphertexts of 0

$p_i = \langle \mathbf{a}_i, \mathbf{s} \rangle + x_i$

$\mathbf{s}$

$(\mathbf{a}, b)$

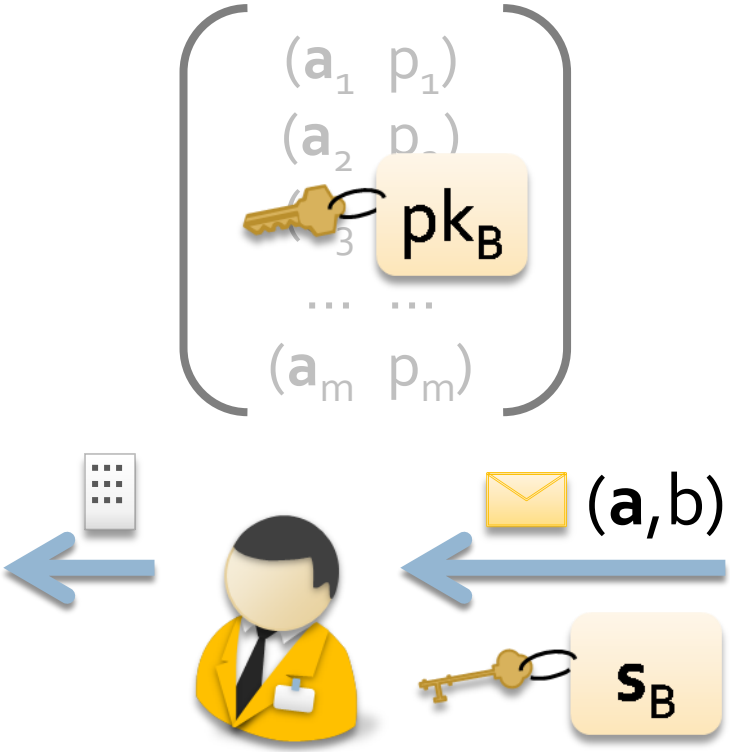
$\mu \in \{0,1\}$

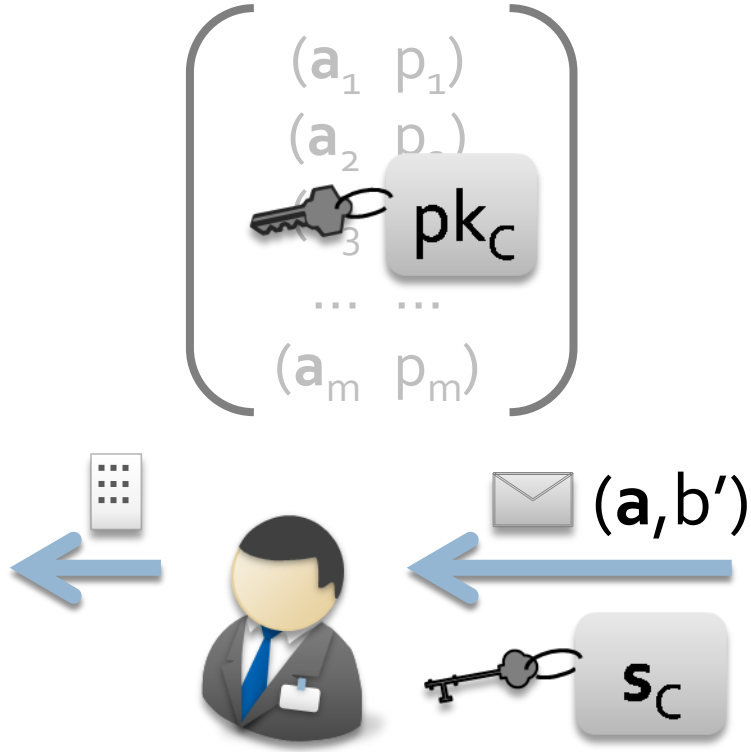
pk_B

$d = b - \langle \mathbf{a}, \mathbf{s} \rangle = \mu q/2 + \Sigma_i r_i x_i$,
$\mu = 0$ if $|d| < q/4$

$\mathbf{r} \leftarrow \{0,1\}^m$, $\mathbf{a} = \Sigma_i r_i \mathbf{a}_i$,
$b = \mu q/2 + \Sigma_i r_i p_i$

LWE-based PKE — Towards PRE

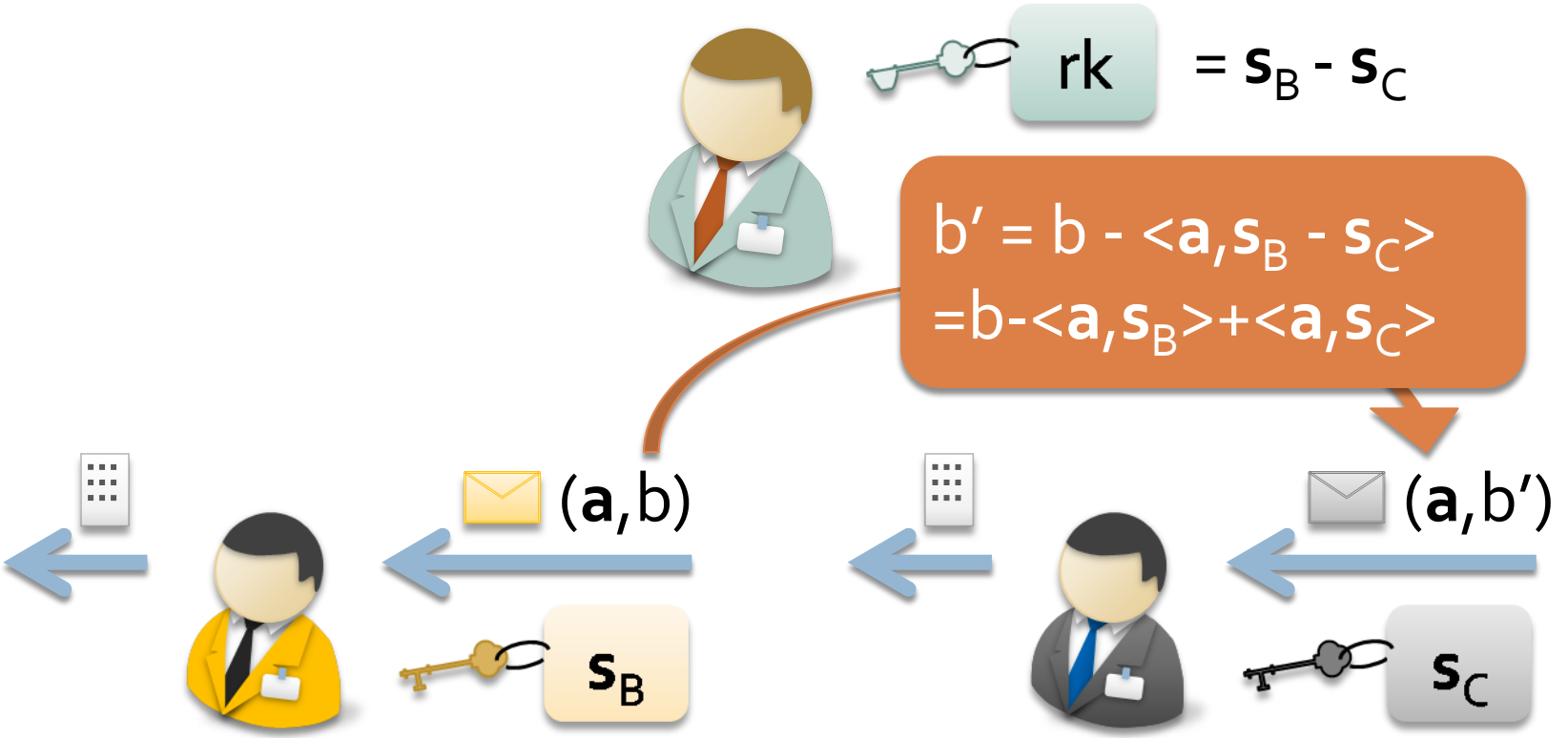




$d=b-\langle \mathbf{a},\mathbf{s}_B\rangle$
$\mu=0$ if $|d|<q/4$

$d=b'-\langle \mathbf{a},\mathbf{s}_C\rangle$
$\mu=0$ if $|d|<q/4$

LWE-based PRE



$d = b - \langle \mathbf{a}, \mathbf{s}_B \rangle$
$\mu = 0$ if $|d| < q/4$

$d = b' - \langle \mathbf{a}, \mathbf{s}_C \rangle = b - \langle \mathbf{a}, \mathbf{s}_B \rangle$
$\mu = 0$ if $|d| < q/4$

Open Problems

- Improvements
  - IND-PRE-CCA2, key anonymity, obfuscation, …
  - efficient PRE (based on ideal lattices)
  - unidirectional PRE
    - Gentry's homomorphic one achieved
- Other constructions
  - from "Dual" PKE and IBE [GPV08]
  - from Peikert-KEM [Pei09]