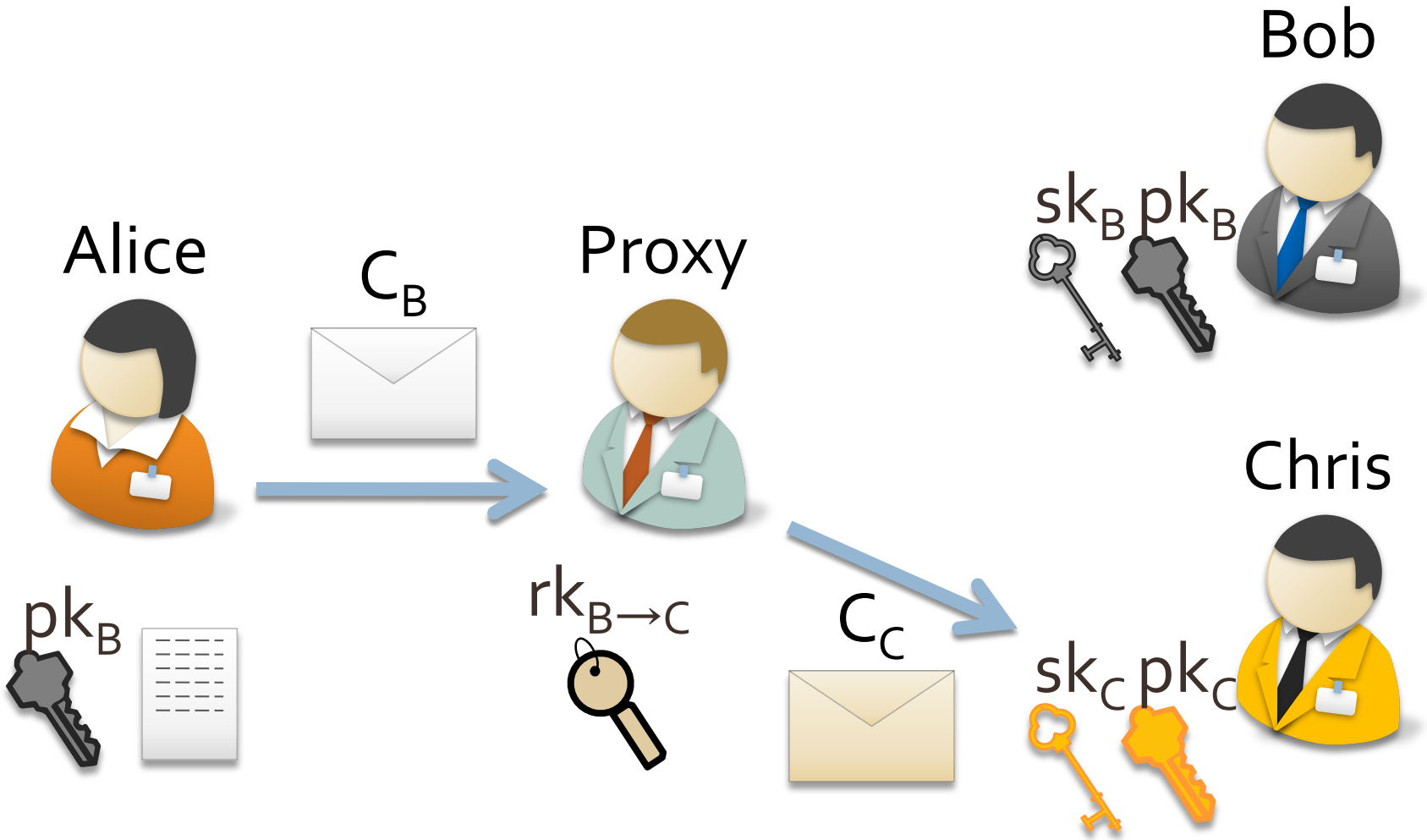
Proxy Re-Encryption from Learning with Errors

Keita Xagawa and Keisuke Tanaka (Tokyo Tech)

Proxy Re-Encryption



DDH and LWE

	DDH	LWE
Lossy TDFs	PW08	PW08
KDM PKE	BHHO08, BGK09, BHHI09	ACPS09, BGK09, BHHI09
KLM PKE	SN09	AGV09
PRE	BBS98	???

Regev's PKE

- KG: $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$, $\mathbf{s} \leftarrow \mathbb{Z}_q^n$, $\mathbf{x} \leftarrow \Psi_\alpha^m$, $\mathbf{p} \leftarrow \mathbf{A}^T\mathbf{s}+\mathbf{x}$
- Enc(w): $e \leftarrow \{0,1\}^m$, $\mathbf{u} \leftarrow \mathbf{A}\mathbf{e}$, $v \leftarrow \mathbf{p}^T\mathbf{e}+w\lfloor q/2 \rfloor$
- Dec($\mathbf{u}$,v): $d \leftarrow v - \mathbf{u}^T\mathbf{s}$,

  $w=0$ if $|d|<q/4$, $w=1$ o.w.

Regev's PKE

- KG: $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$, $\mathbf{s} \leftarrow \mathbb{Z}_q^n$, $\mathbf{x} \leftarrow \Psi_\alpha^m$, $\mathbf{p} \leftarrow \mathbf{A}^T\mathbf{s}+\mathbf{x}$
- Enc(w): $e \leftarrow \{0,1\}^m$, $\mathbf{u} \leftarrow \mathbf{A}\mathbf{e}$, $v \leftarrow \mathbf{p}^T\mathbf{e}+w\lfloor q/2 \rfloor$
- Dec($\mathbf{u}$,v): $d \leftarrow v - \mathbf{u}^T\mathbf{s}$,

  w=0 if $|d|<q/4$, w=1 o.w.

$dLWE_{q,m,\alpha}$

$$O_A^m \rightarrow (\mathbf{A}^T, \mathbf{A}^T\mathbf{s}+\mathbf{x}) \approx_c (\mathbf{A}^T, \mathbf{z}) \leftarrow U(\mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^m)$$

If we replace a key ($\mathbf{A}^T$, $\mathbf{p}$) with ($\mathbf{A}^T$, $\mathbf{z}$),

the ciphertext ($\mathbf{u}$, v) contains no information of w.

1st PRE based on Regev's PKE

- KG: $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$, $\mathbf{s} \leftarrow \mathbb{Z}_q^n$, $\mathbf{x} \leftarrow \Psi_\alpha^m$, $\mathbf{p} \leftarrow \mathbf{A}^T\mathbf{s}+\mathbf{x}$
- Enc(w): $e \leftarrow \{0,1\}^m$, $\mathbf{u} \leftarrow \mathbf{Ae}$, $v \leftarrow \mathbf{p}^T\mathbf{e}+w\lfloor q/2 \rfloor$
- Dec($\mathbf{u}$,v): $d \leftarrow v - \mathbf{u}^T\mathbf{s}$,

  w=0 if $|d|<q/4$, w=1 o.w.
- ReKey: $\mathbf{R}_{ij}\,\mathbf{s}_i = \mathbf{s}_j$, where $\mathbf{R}_{ij}$ is a GF(q^n)-matrix
- ReEnc($\mathbf{u}$,v): $(\mathbf{u}', v) \leftarrow (\mathbf{R}_{ij}^{-T}\mathbf{u}, v)$

1st PRE based on Regev's PKE

- KG: $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$, $\mathbf{s} \leftarrow \mathbb{Z}_q^n$, $\mathbf{x} \leftarrow \Psi_\alpha^m$, $\mathbf{p} \leftarrow \mathbf{A}^T\mathbf{s}+\mathbf{x}$
- Enc(w): $e \leftarrow \{0,1\}^m$, $\mathbf{u} \leftarrow \mathbf{A}\mathbf{e}$, $v \leftarrow \mathbf{p}^T\mathbf{e}+w\lfloor q/2 \rfloor$
- Dec($\mathbf{u}$,v): $d \leftarrow v - \mathbf{u}^T\mathbf{s}$,

  $w=0$ if $|d|<q/4$, $w=1$ o.w.
- ReKey: $\mathbf{R}_{ij}\,\mathbf{s}_i = \mathbf{s}_j$, where $\mathbf{R}_{ij}$ is a GF(q^n)-matrix
- ReEnc($\mathbf{u}$,v): $(\mathbf{u}', v) \leftarrow (\mathbf{R}_{ij}^{-T}\mathbf{u}, v)$
- Notes
  - #1: $d_i = v - \mathbf{u}^T\mathbf{s}_i = v - \mathbf{u}^T\mathbf{R}^{-1}\,\mathbf{R}\mathbf{s}_i = v - (\mathbf{R}^{-T}\mathbf{u})^T\mathbf{s}_j = d_j$
  - #2: $(wg^k, g^{ak}) \rightarrow (wg^k, g^{bk})$ if you know a/b [BBS98]

Proof Idea

$\mathbf{A}_i^T$, $\mathbf{p}_i = \mathbf{A}_i^T \mathbf{s}_i + \mathbf{x}_i$
$\mathbf{R}_{ij}\ \mathbf{s}_i = \mathbf{s}_j$

Game0

$\tilde{\mathbf{A}}_i^T$, $\mathbf{p}_i = \tilde{\mathbf{A}}_i^T \mathbf{s} + \mathbf{x}_i$
$\mathbf{R}_{oi} \leftarrow GF(q^n)$
$\mathbf{A}_i^T \leftarrow \tilde{\mathbf{A}}_i^T \mathbf{R}_{oi}^{-1}$

Game1

$\tilde{\mathbf{A}}_i^T$, $\mathbf{r}_i$
$\mathbf{R}_{oi} \leftarrow GF(q^n)$
$\mathbf{A}_i^T \leftarrow \tilde{\mathbf{A}}_i^T \mathbf{R}_{oi}^{-1}$

Game2

Perfect

$dLWE_{q,(Q+1)m,\alpha}$

Conclusion

	Plaintext	Params	q	α
1st	Single/Multi	-	poly	1/poly
2nd	Multi	-	QP	1/poly
3rd	Multi	A	QP	1/QP
IBE	Single	A	QP	1/QP

Open Problems:
IND-CCA2, IdealLWE-based, IBE w/o RO, etc