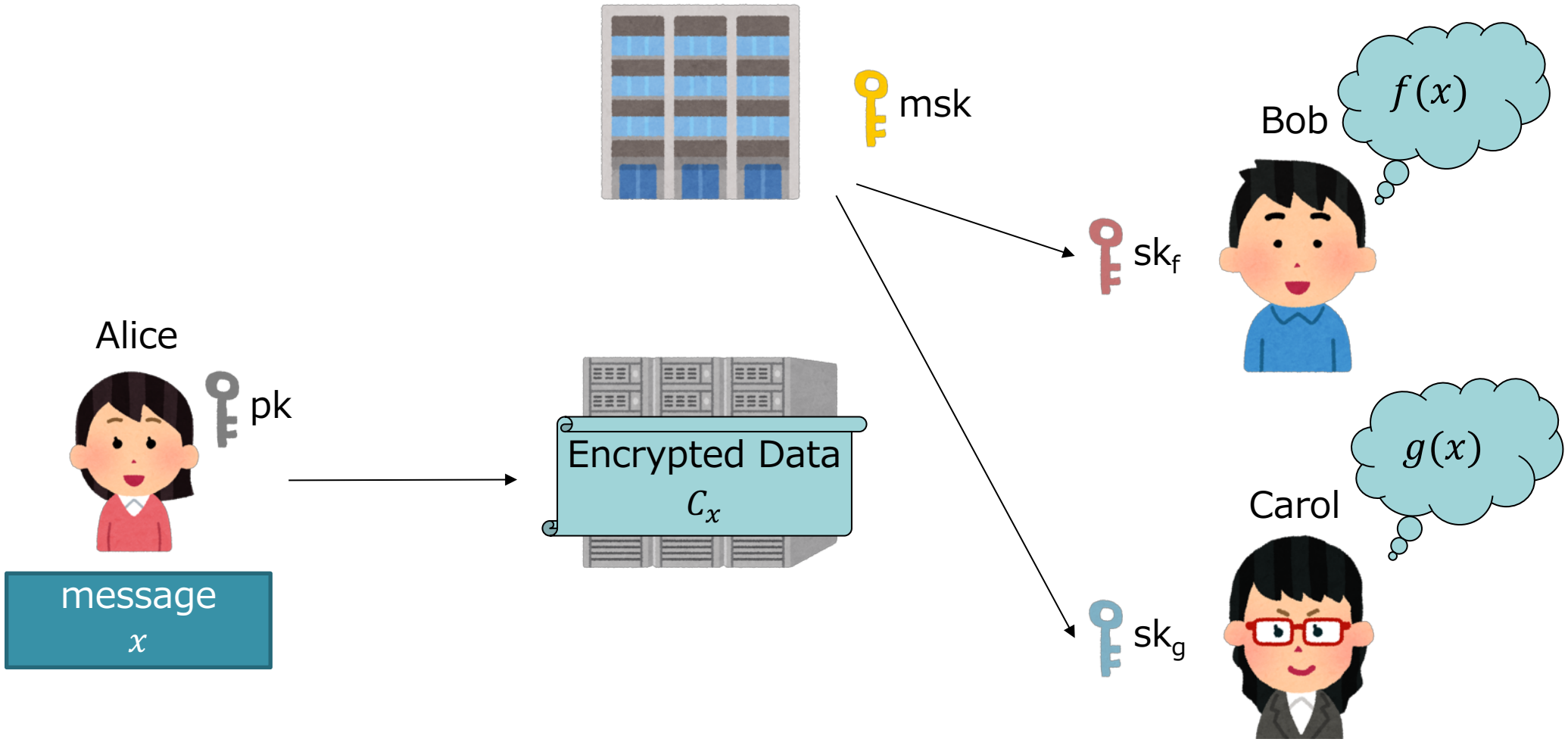
Unbounded Inner Product Functional Encryption from Bilinear Maps

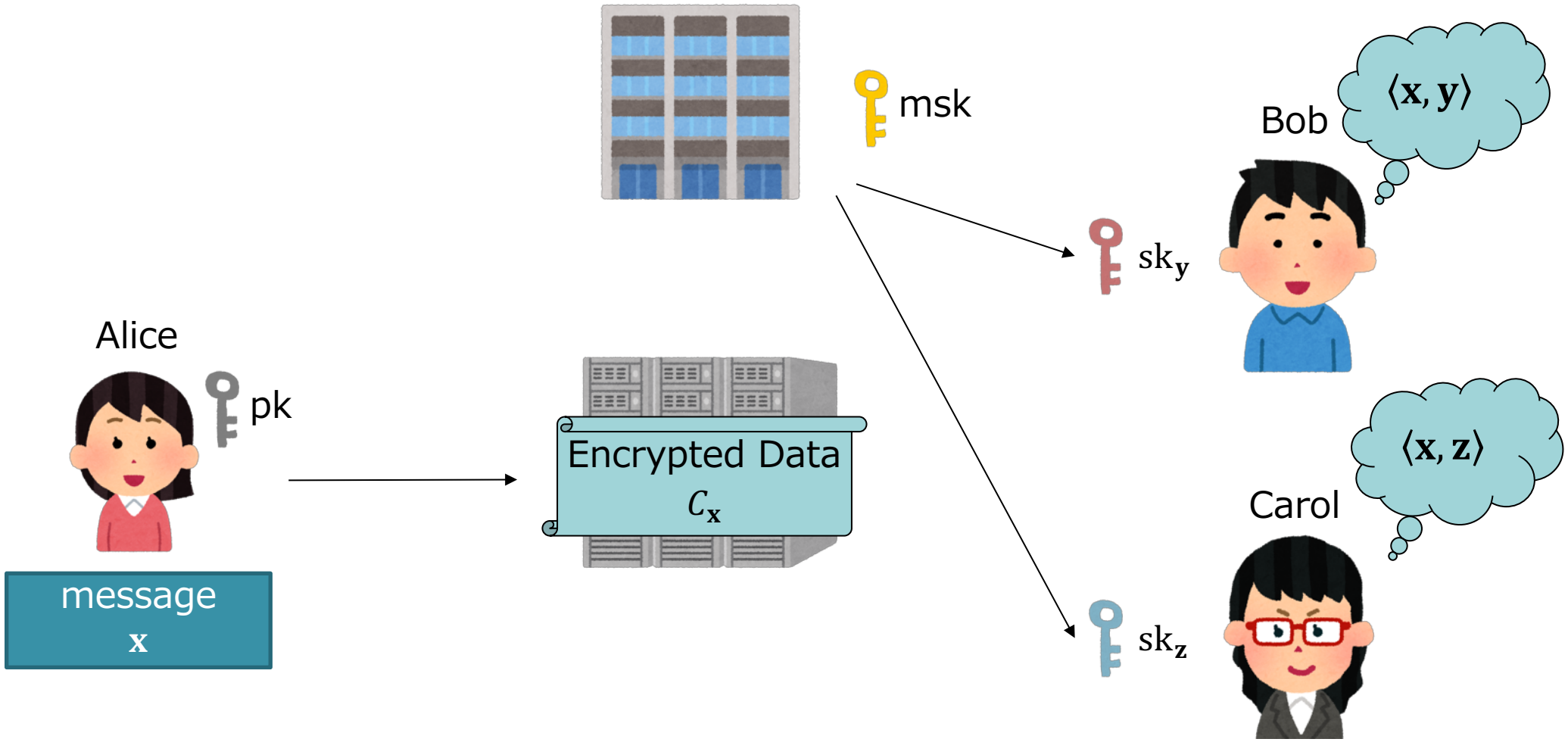
ASIACRYPT 2018

Junichi Tomida (NTT), Katsuyuki Takashima (Mitsubishi Electric)

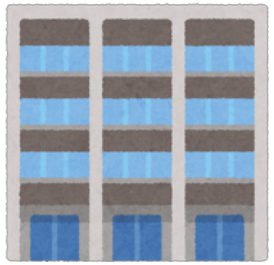
Functional Encryption[O'Neill10, BSW11]



Inner Product Functional Encryption (IPFE)[ABDP15]



Application of IPFE (DNA Sequence Similarity)



msk

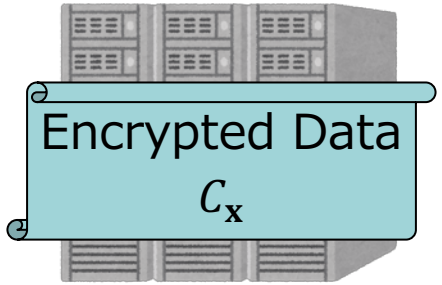
pk

Vector for (A, C, T)
$\mathbf{y} = (1,0,0,0,0,0,1,0,0,0,0,1)$

$\mathrm{sk}_{\mathbf{y}}$

Encoding

$A = (1,0,0,0)$
$G = (0,1,0,0)$
$C = (0,0,1,0)$
$T = (0,0,0,1)$

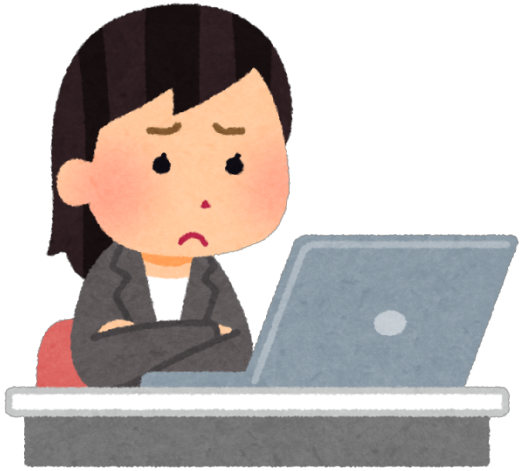


Vector for (A, T, T)
$\mathbf{x} = (1,0,0,0,0,0,0,1,0,0,0,1)$

$\langle \mathbf{x}, \mathbf{y} \rangle = 2$

Motivation of This Work

- **All known IPFE schemes require to determine the vector length at the deployment phase.**
- **What kind of data will be handled? DNA sequences for the first chromosome? For humans? Or for all Species?**
- **Difficult to determine the length at the deployment phase.**
  - Too large: efficiency loss
  - Too small: redeployment



Main Results of This Work

✓ **Unbounded IPFE for both private-key and public-key setting.**

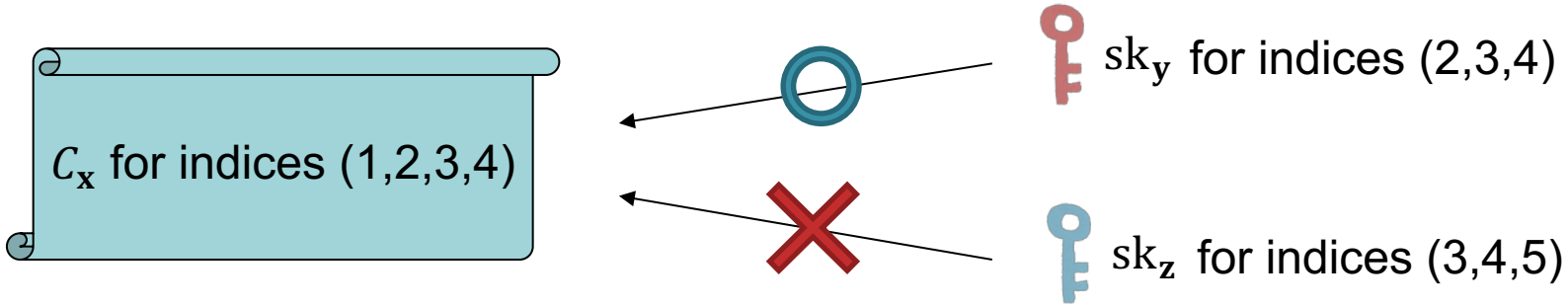
- Can handle any lengths of vectors for encryption and key generation.
- Secure under the standard model and a standard assumption.
- The former has function privacy. $\mathrm{sk}_{\mathbf{y}}$ hides the information of $\mathbf{y}$.

- **How to define the decryption?**
  - There are ciphertexts and secret keys of various lengths.

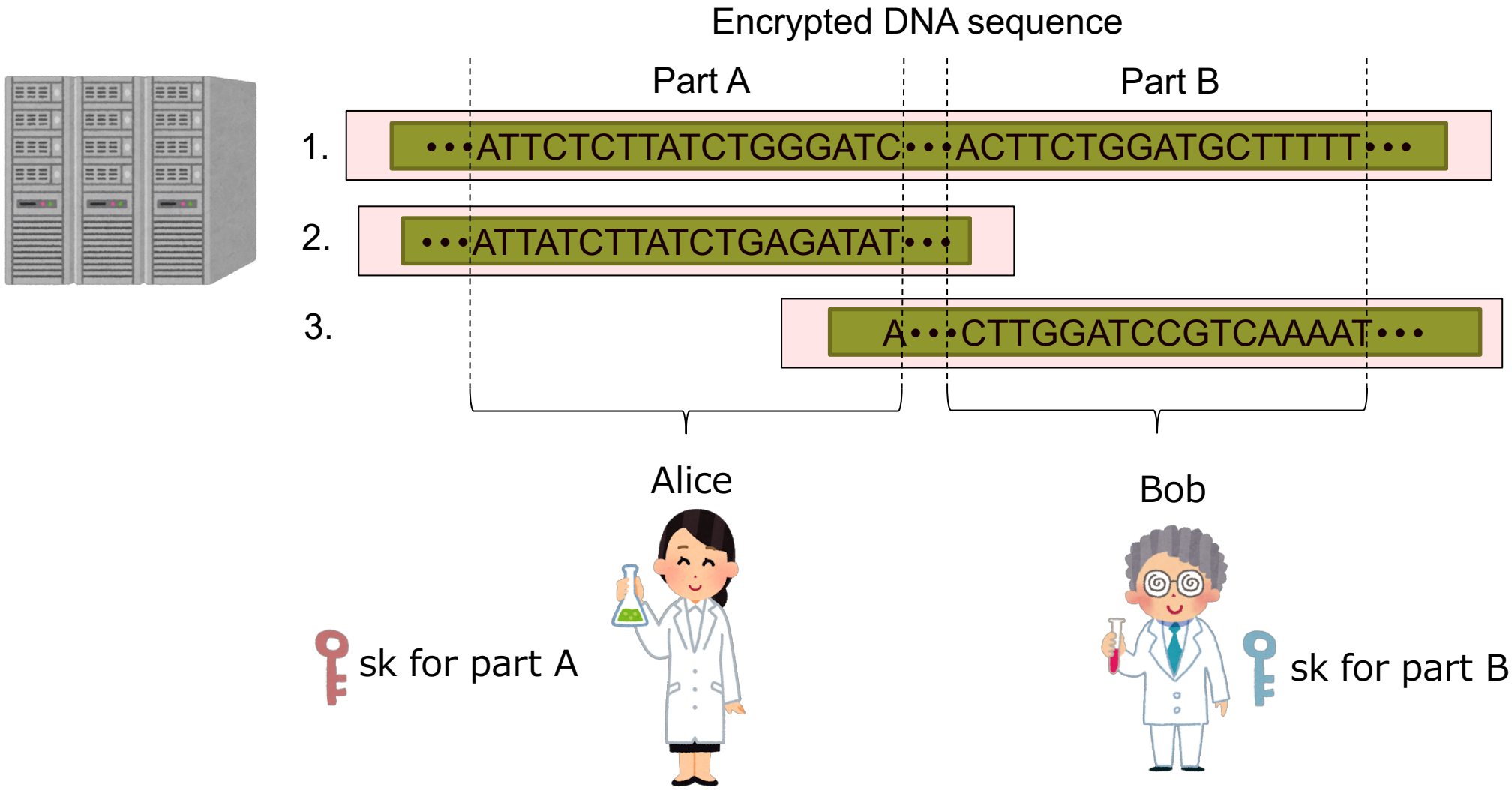
Main Results of This Work

✓ **Allowing partial decryption.**

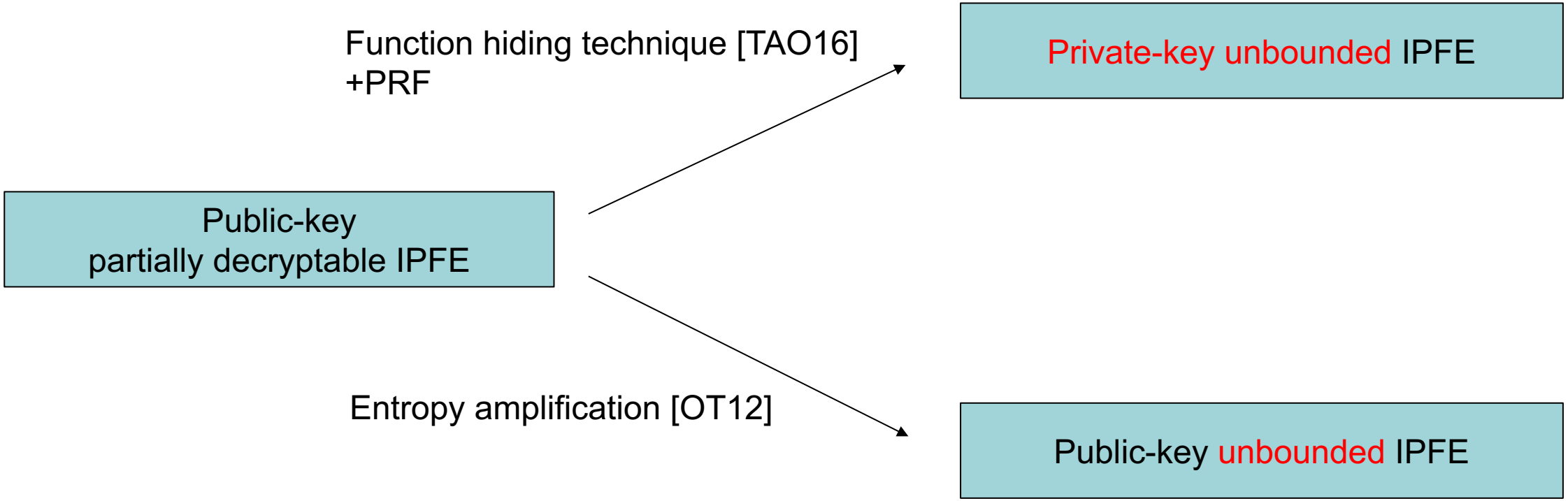
- A ciphertext for indexed vector $\mathbf{x} \in \mathbb{Z}^{S_c}$ can be decrypted with a secret key for indexed vector $\mathbf{y} \in \mathbb{Z}^{S_k}$ iff $S_c \supseteq S_k$.
- It seems inconvenient if decryption is possible only when the lengths of a ciphertext and a secret key are the same.



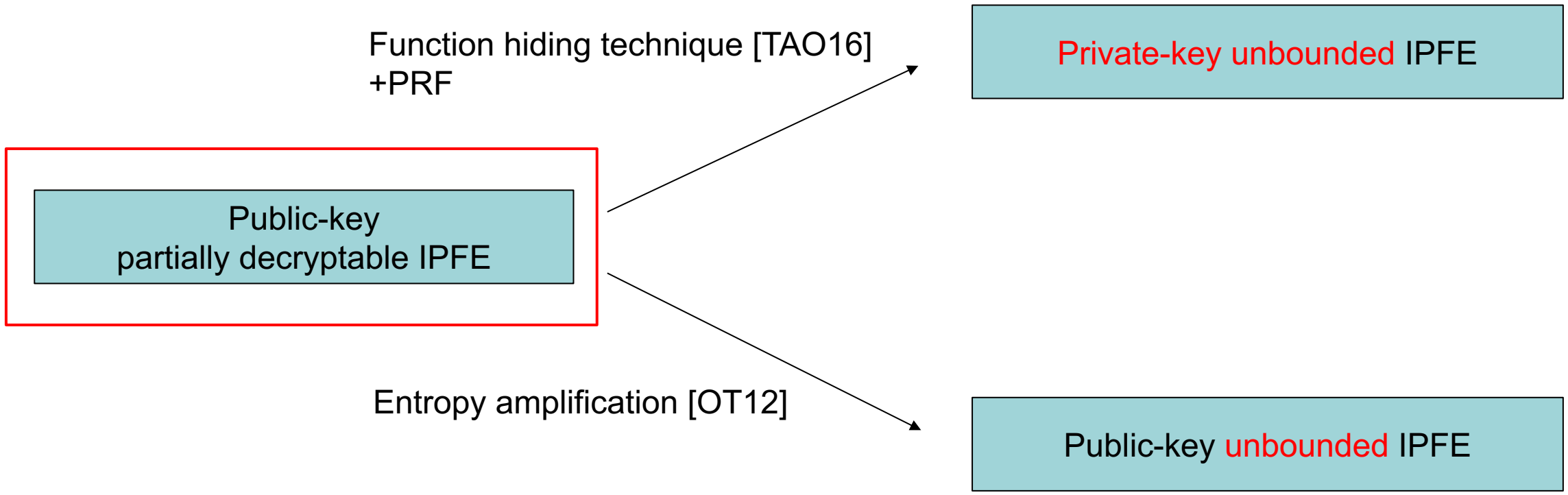
Why Partial Decryption?: $S_c \supseteq S_k$



Roadmap



Roadmap



Partially Decryptable IPFE

- $\mathrm{Setup}(1^\lambda, 1^m) \to \mathrm{pk}, \mathrm{msk}$
- $\mathrm{Enc}(\mathrm{pk}, \mathbf{x}) \to \mathrm{ct}$
- $\mathrm{KeyGen}(\mathrm{msk}, \mathbf{y}) \to \mathrm{sk}$
- $\mathrm{Dec}(\mathrm{ct}, \mathrm{sk}) \to d \ or \ \perp$

Normal IPFE

$\mathbf{x}, \mathbf{y} \in \mathbb{Z}^m$

$d = \langle \mathbf{x}, \mathbf{y} \rangle$ over $\mathbb{Z}$

Partially decryptable IPFE

$\mathbf{x} \in \mathbb{Z}^{S_c}, \mathbf{y} \in \mathbb{Z}^{S_k}$ for any $S_c, S_k \subseteq [m] = \{1, \dots, m\}$

$d = \sum_{i \in S_k} x_i y_i$ over $\mathbb{Z}$ iff $S_c \supseteq S_k$.

Extension of Function Class

Normal IPFE

$$f_{\mathbf{y}}: \mathbb{Z}^m \to \mathbb{Z} \text{ s.t. } f_{\mathbf{y}}(\mathbf{x}) = \langle \mathbf{x}, \mathbf{y} \rangle$$

Partially decryptable IPFE

$$f_{\mathbf{y},S_k}: \bigcup_{S \subseteq [m]} \mathbb{Z}^S \to \mathbb{Z} \text{ s.t. } f_{\mathbf{y},S_k}(\mathbf{x}, S_c) = \begin{cases} \sum_{i \in S_k} x_i y_i & \text{if } S_c \supseteq S_k \\ \perp & \text{otherwise} \end{cases}$$

Security of Partially Decryptable IPFE

Adversary

b'

pk

$(\mathbf{y}_i, S_{k,i})$

$\mathrm{sk} = \mathrm{KeyGen}(\mathrm{msk}, \mathbf{y}_i)$

$(\mathbf{x}_0, \mathbf{x}_1, S_c)$

$C_b = \mathrm{Enc}(\mathrm{pk}, \mathbf{x}_b)$

⋮

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

Challenger

Condition

For $\mathbf{x}_0, \mathbf{x}_1 \in \mathbb{Z}^{S_c}$, $\mathbf{y}_i \in \mathbb{Z}^{S_{k,i}}$,
$\forall i, \sum_{j \in S_{k,i}} x_{0,j} y_j = \sum_{j \in S_{k,i}} x_{1,j} y_j$ when $S_c \supseteq S_{k,i}$.

Colluded illegitimate keys (i,.e. $S_c \not\supseteq S_{k,i}$) are useless for decryption.

Construction of Partially Decryptable IPFE

- **Normal IPFE scheme (not secure).**
  - $\mathrm{Setup} \rightarrow \mathrm{pk} = [\mathbf{B}]_1, \mathrm{msk} = \mathbf{B}^* = (\mathbf{B}^\top)^{-1}$, where $\mathbf{B} \leftarrow \mathbb{Z}_p^{m \times m}$
  - $\mathrm{Enc}(\mathrm{pk}, \mathbf{x}) \rightarrow [\mathbf{x}\mathbf{B}]_1$
  - $\mathrm{KeyGen}(\mathrm{msk}, \boldsymbol{y}) \rightarrow [\mathbf{y}\mathbf{B}^*]_2$
  - $\mathrm{Dec}(\mathrm{ct}, \mathrm{sk}) \rightarrow e([\mathbf{x}\mathbf{B}]_1, [\mathbf{y}\mathbf{B}^*]_2) = [\langle \mathbf{x}, \mathbf{y} \rangle]_T$

- $[\mathbf{M}]_i = \boldsymbol{g}_i^{\mathbf{M}} = \left(\boldsymbol{g}_i^{m_{j,\ell}}\right)_{j \in [m], \ell \in [n]}$

Construction of Partially Decryptable IPFE

$\mathrm{Setup}(1^m)$	$(\mathrm{pk}_1, \mathrm{msk}_1)$	$(\mathrm{pk}_2, \mathrm{msk}_2)$	.....	$(\mathrm{pk}_m, \mathrm{msk}_m)$	Normal IPFE scheme for 2 dimensions
$\mathrm{Enc}(\mathbf{x}, S_c)$	(x_1, z)	(x_2, z)	.....	(x_m, z)	For $i \in [S_c]$
$\mathrm{KeyGen}(\mathbf{y}, S_k)$	(y_1, r_i)		.....	(y_m, r_m)	For $i \in [S_k]$, $\sum_{i \in S_k} r_i = 0$

Dec

$$d = \sum_{i \in S_k} \mathrm{Dec}(\mathrm{ct}_i, \mathrm{sk}_i) = \sum_{i \in S_k} x_i y_i + \underline{z r_i} = \sum_{i \in S_k} x_i y_i$$

This part seems pseudorandom by SXDH when $S_c \not\supseteq S_k$, preventing collusion attack.
But what the adversary obtains are ct and sk...

Comparison with Bounded Schemes

(Function-Hiding) Private-Key IPFE					
Reference	|msk|	|ct|	|sk|	Pairing	Assumption
DDM16	$(8m^2 + 12m + 28)\|\mathbb{Z}_p\|$	$(4m + 8)\|G_1\|$	$(4m + 8)\|G_2\|$	Yes	SXDH
TAO16	$(4m^2 + 18m + 20)\|\mathbb{Z}_p\|$	$(2m + 5)\|G_1\|$	$(2m + 5)\|G_2\|$	Yes	XDLIN
KKS17	$(6m + 8)\|\mathbb{Z}_p\|$	$(2m + 8)\|G_1\|$	$(2m + 8)\|G_2\|$	Yes	SXDH
Ours	|PRF key|	$4m\|G_1\|$	$4m\|G_2\|$	Yes	SXDH

Public-Key IPFE						
Reference	|pk|	|msk|	|ct|	|sk|	Pairing	Assumption
ALS16	$(m + 1)\|G\|$	$(m + 1)\|\mathbb{Z}_p\|$	$(2m + 1)\|G\|$	$2\|\mathbb{Z}_p\|$	No	DDH
Ours	$28\|G_1\|$	$28\|\mathbb{Z}_p\|$	$7m\|G_1\|$	$7m\|G_2\|$	Yes	SXDH

m: vector length

Remark

- In our paper, we directly construct unbounded IPFE schemes essentially utilizing properties of bilinear groups.
- The notion, “Partial decryptable IPFE”, does not appear in our paper.

Conclusion

- **Construction of unbounded IPFE schemes for both public and private-key setting.**
  - Secure under the SXDH assumption in the standard model.
  - Almost the same efficiency as previous private-key IPFE schemes.
- **It provides flexible decryption (partial decryption).**
  - Decryptable iff $S_c \supseteq S_k$.

Thank you for your attention