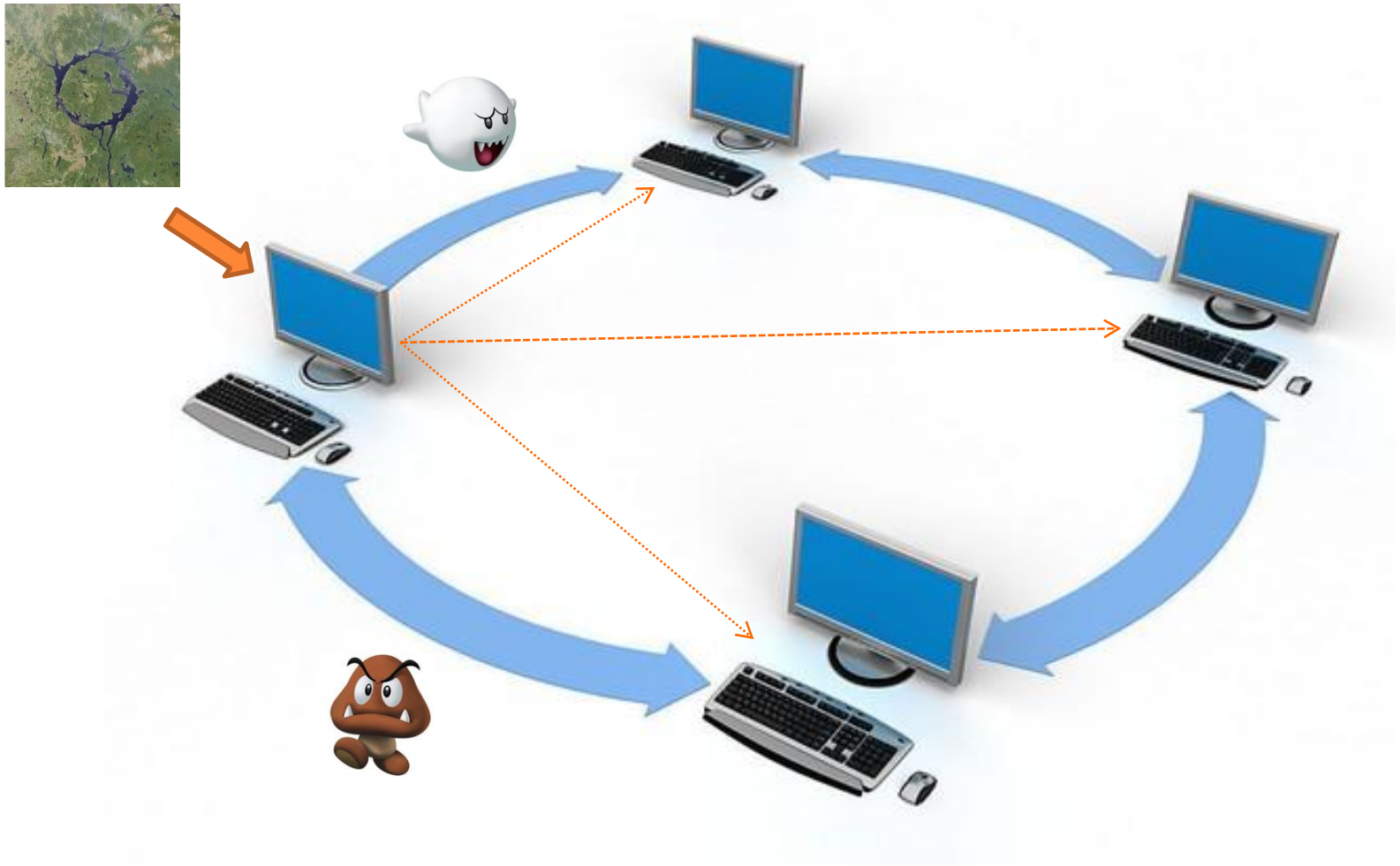
Image Encryption System Based on Self-correlation Permutation

Liang Zhao *† Kouichi Sakurai *
(趙　亮、櫻井　幸一)
*Dept. of Computer Science and Communication Engineering, Kyushu University, Japan
†College of Computer Science, Chongqing University, China

The first author is supported by the governmental scholarship from China Scholarship Council (中国奨学金委員会).
supported by Strategic Japanese-Indian Cooperative Programme on Multidisciplinary Research Field, which combines Information and Communications Technology with Other Fields Supported by Japan Science and Technology Agency and Department of Science and Technology of the Government of India

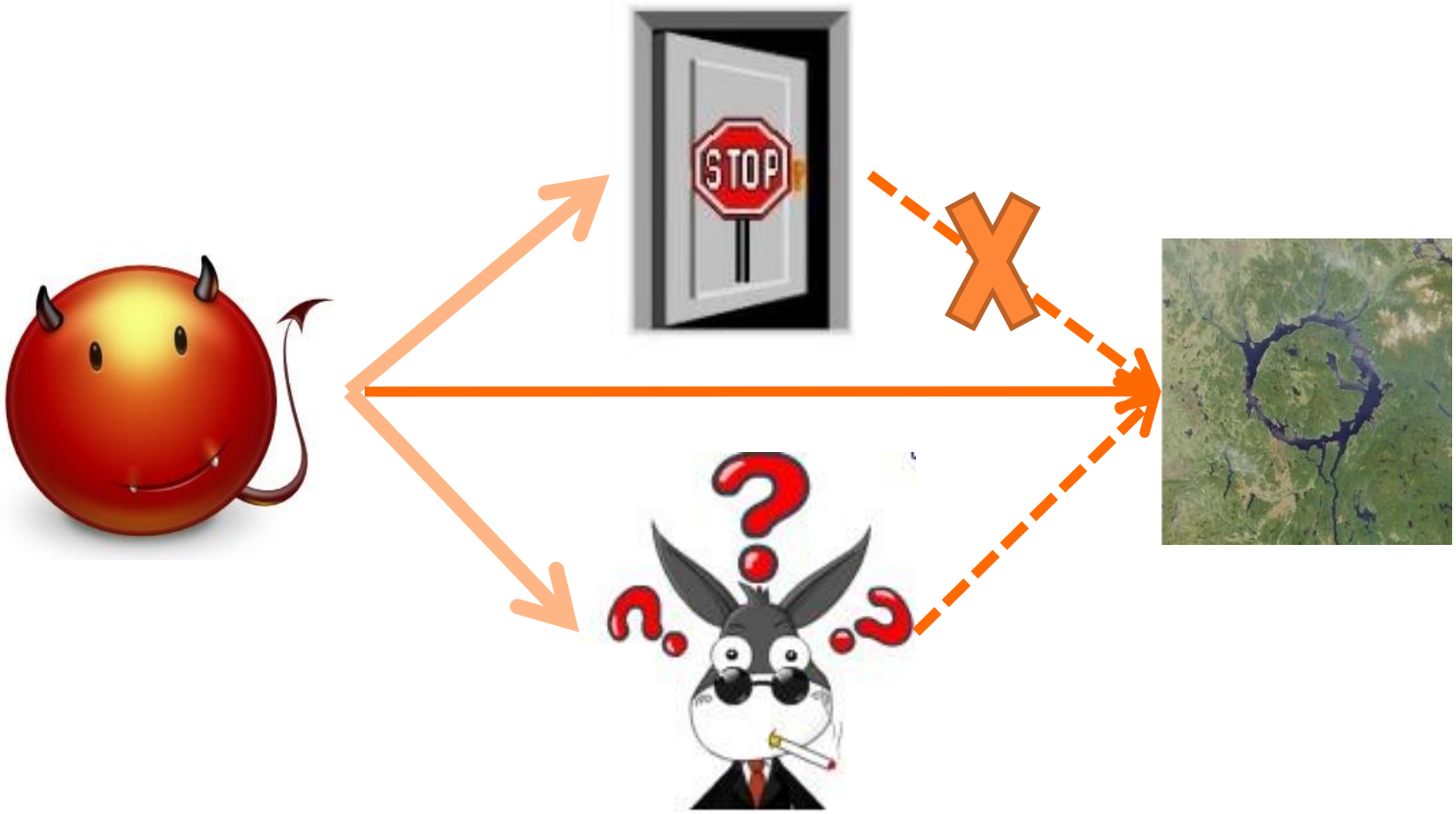
zhaoliang@itslab.csce.kyushu-u.ac.jp

Introduction on image encryption



zhaoliang@itslab.csce.kyushu-u.ac.jp

INTRODUCTION ON IMAGE ENCRYPTION



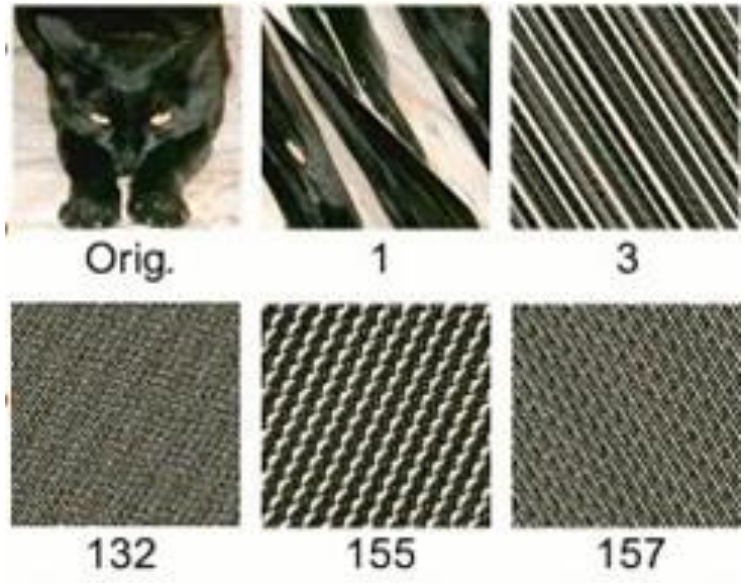
zhaoliang@itslab.csce.kyushu-u.ac.jp

INTRODUCTION ON IMAGE ENCRYPTION

Security of image data

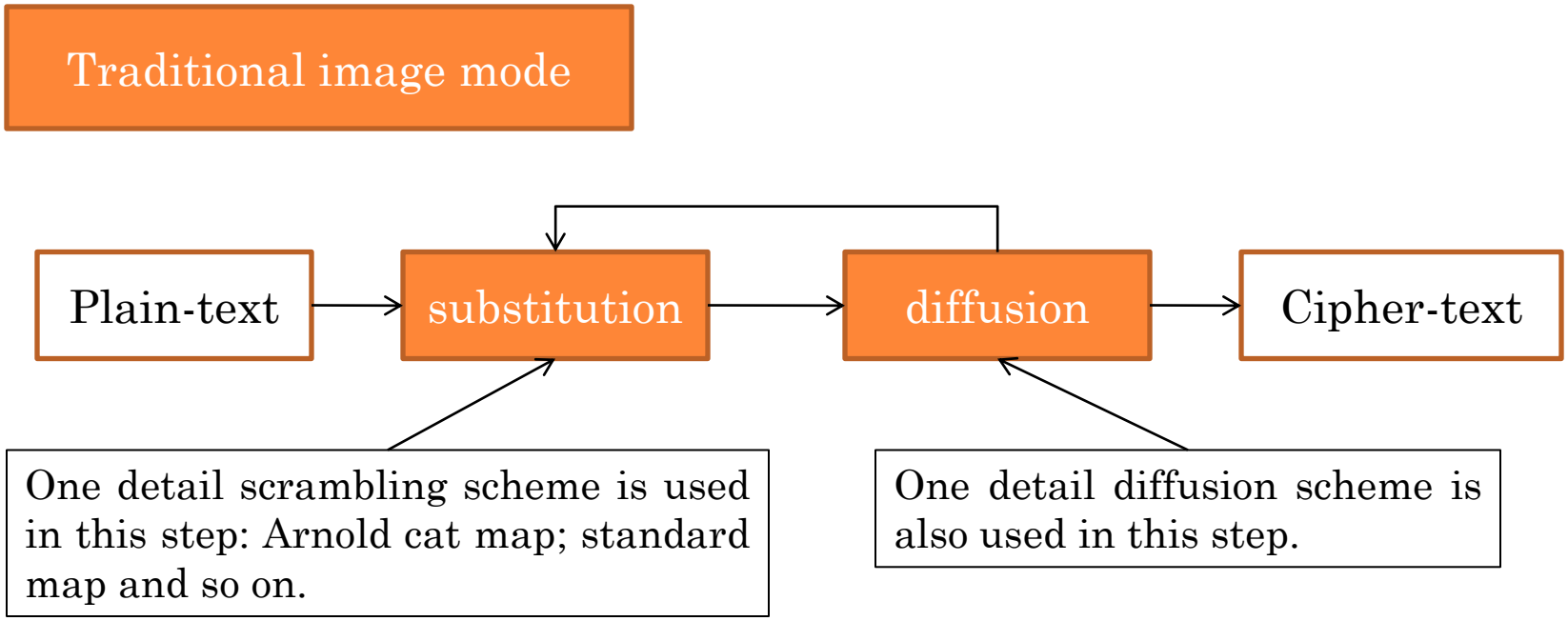
- Characters of image data
- Drawbacks of tradition cipher

Generalized Arnold cat map



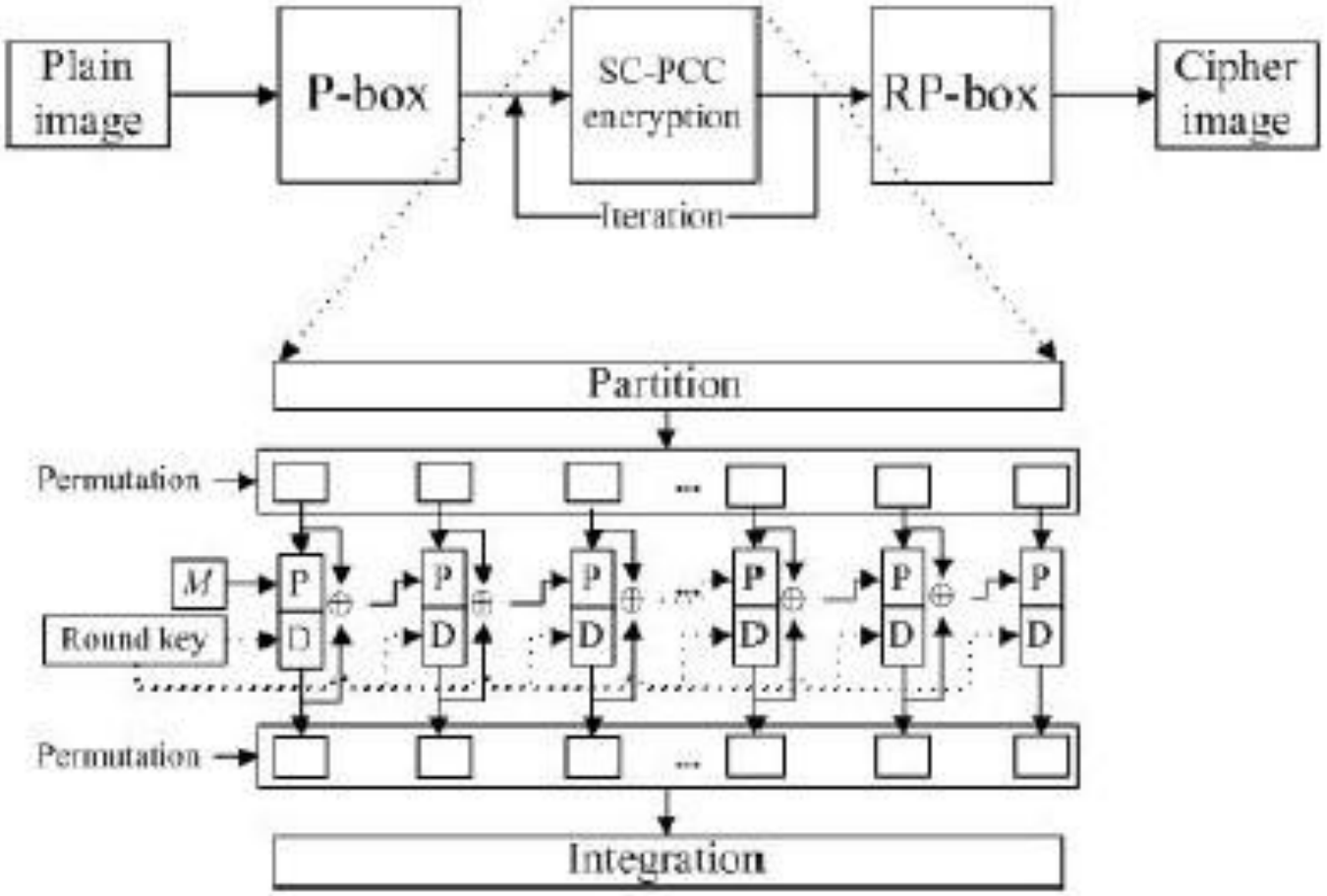
zhaoliang@itslab.csce.kyushu-u.ac.jp

SC-PCC Framework



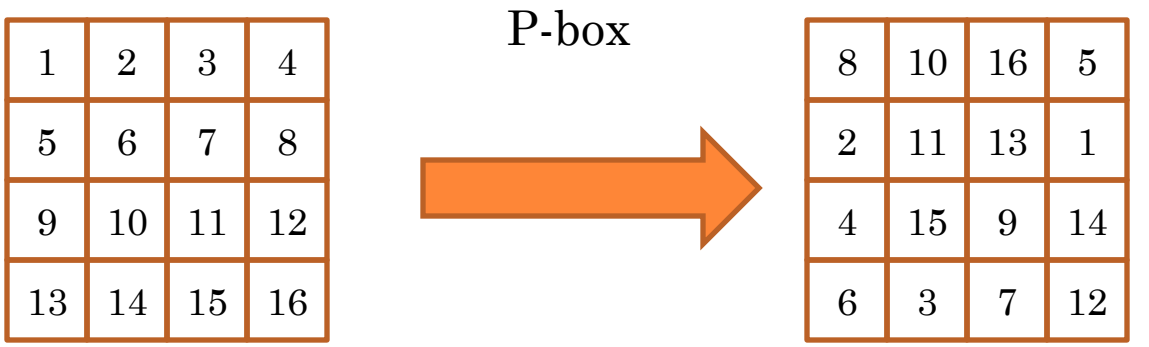
zhaoliang@itslab.csce.kyushu-u.ac.jp

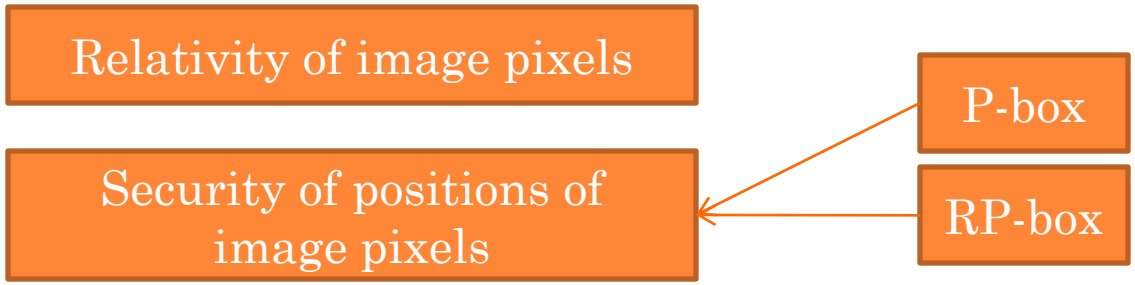
SC-PCC Framework



zhaoliang@itslab.csce.kyushu-u.ac.jp

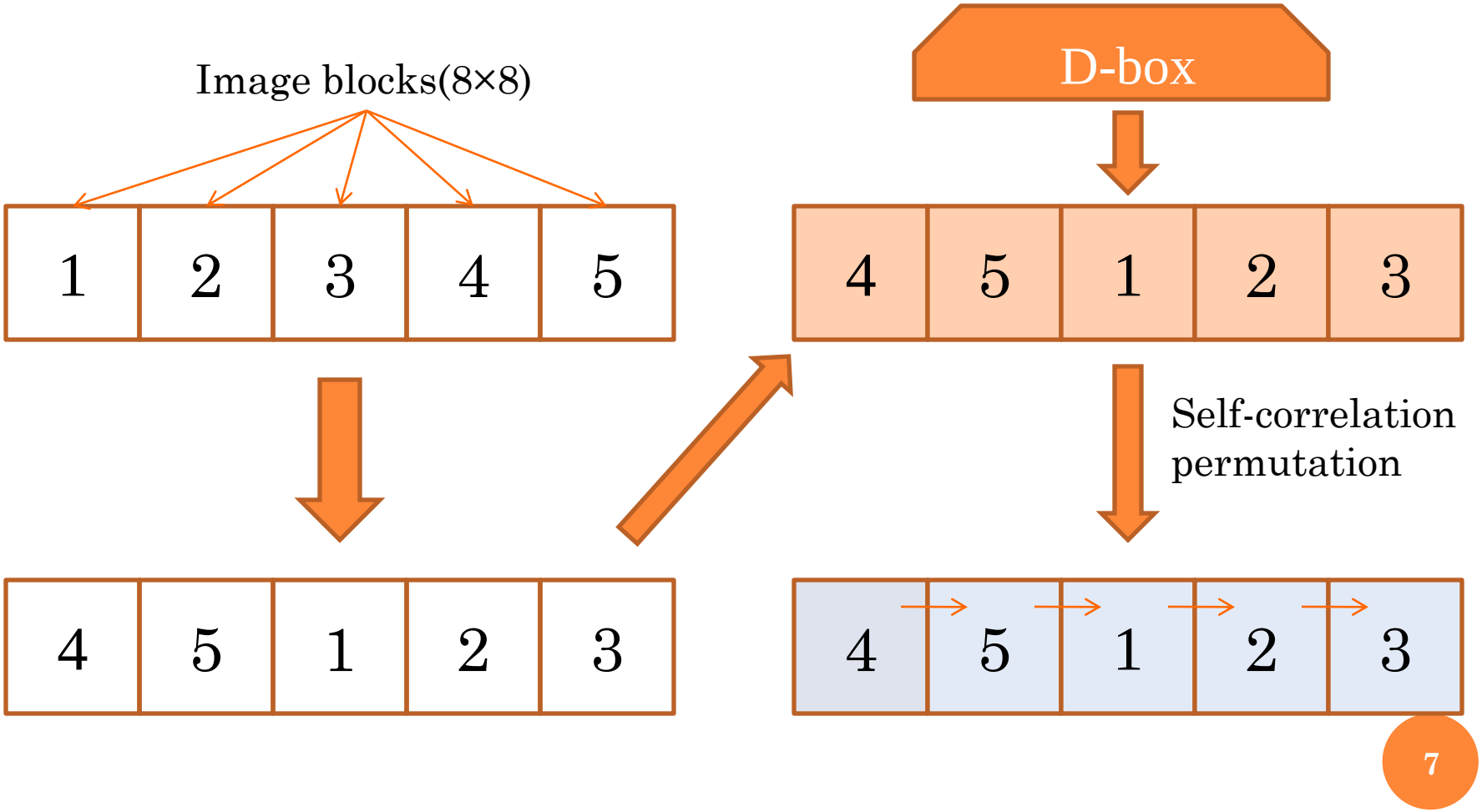
SC-PCC Framework





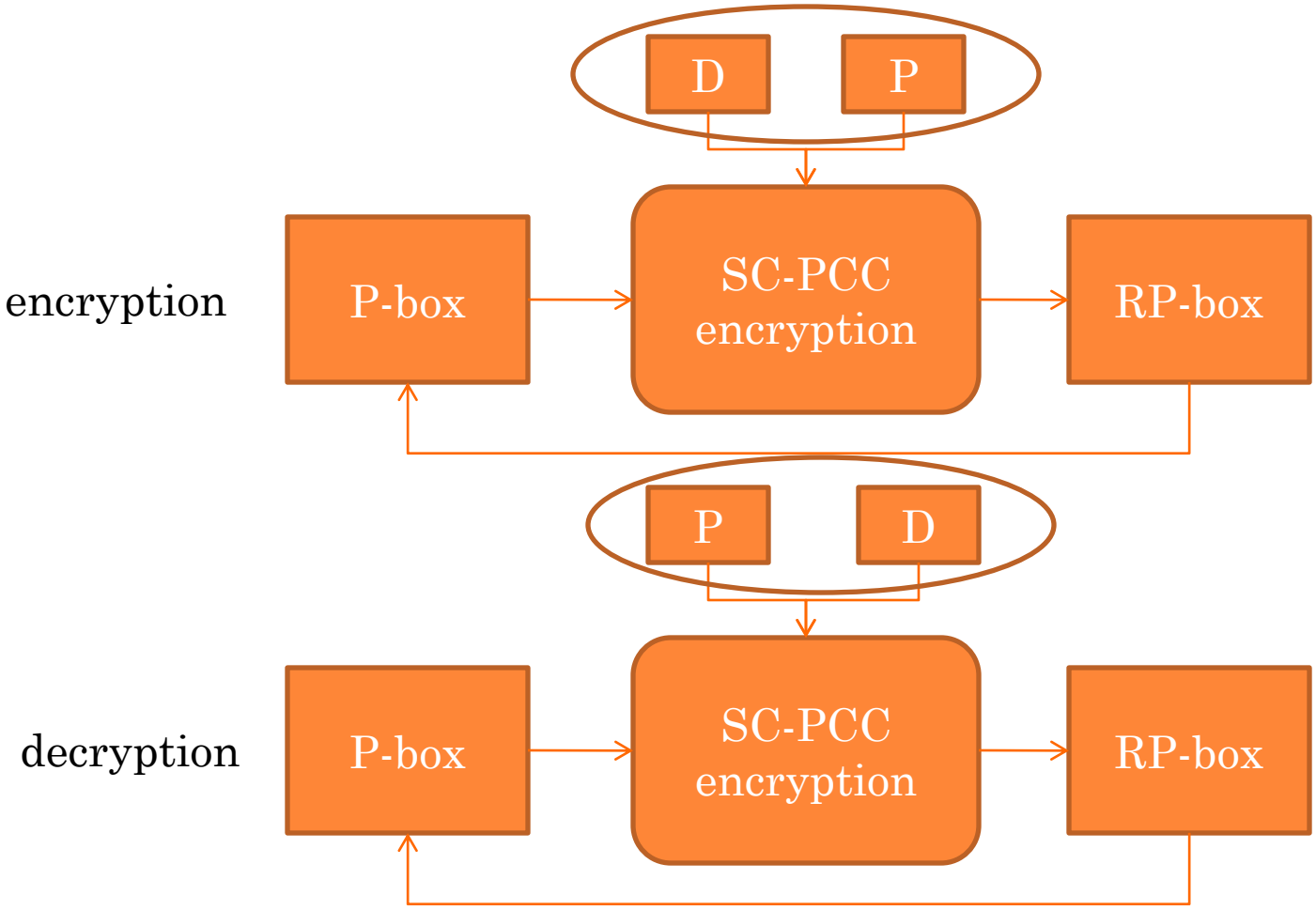
zhaoliang@itslab.csce.kyushu-u.ac.jp

SC-PCC Framework



zhaoliang@itslab.csce.kyushu-u.ac.jp

SC-PCC Framework



zhaoliang@itslab.csce.kyushu-u.ac.jp

Image Encryption Based on SC-PCC Framework

- P-box and RP-box:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N$$

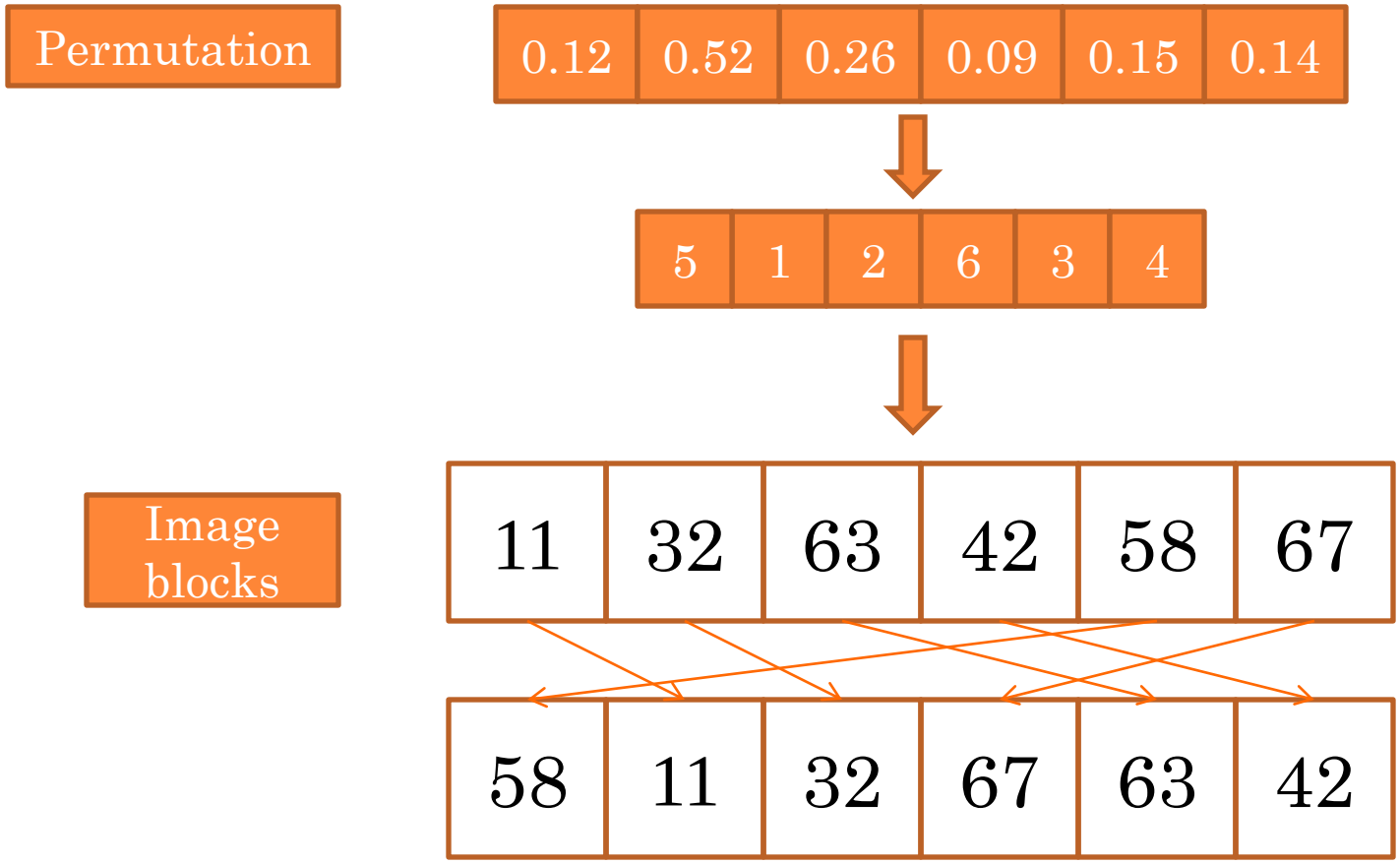
- Random number generation:

$$x_{t+1}^i = (1-\varepsilon)g(x_t^i) + \varepsilon g(x_t^{i-1})$$

$$x_{t+1}^i = \begin{cases} x_t^i/q^i, & x_t^i \in (0, q^i) \\ (1-x_t^i)/(1-q^i), & x_t^i \in [q^i, 1) \end{cases}$$

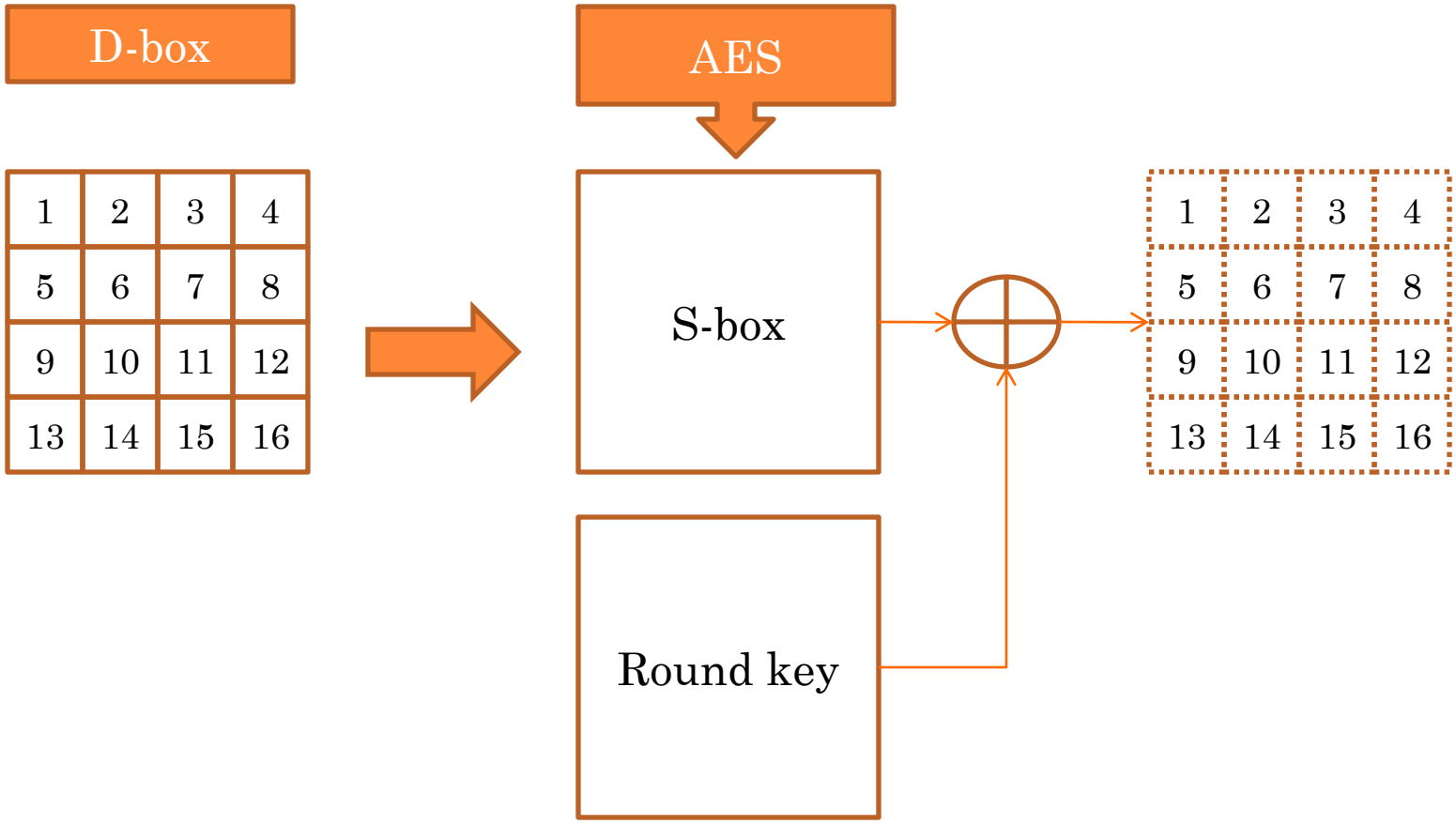
zhaoliang@itslab.csce.kyushu-u.ac.jp

IMAGE ENCRYPTION BASED ON SC-PCC FRAMEWORK



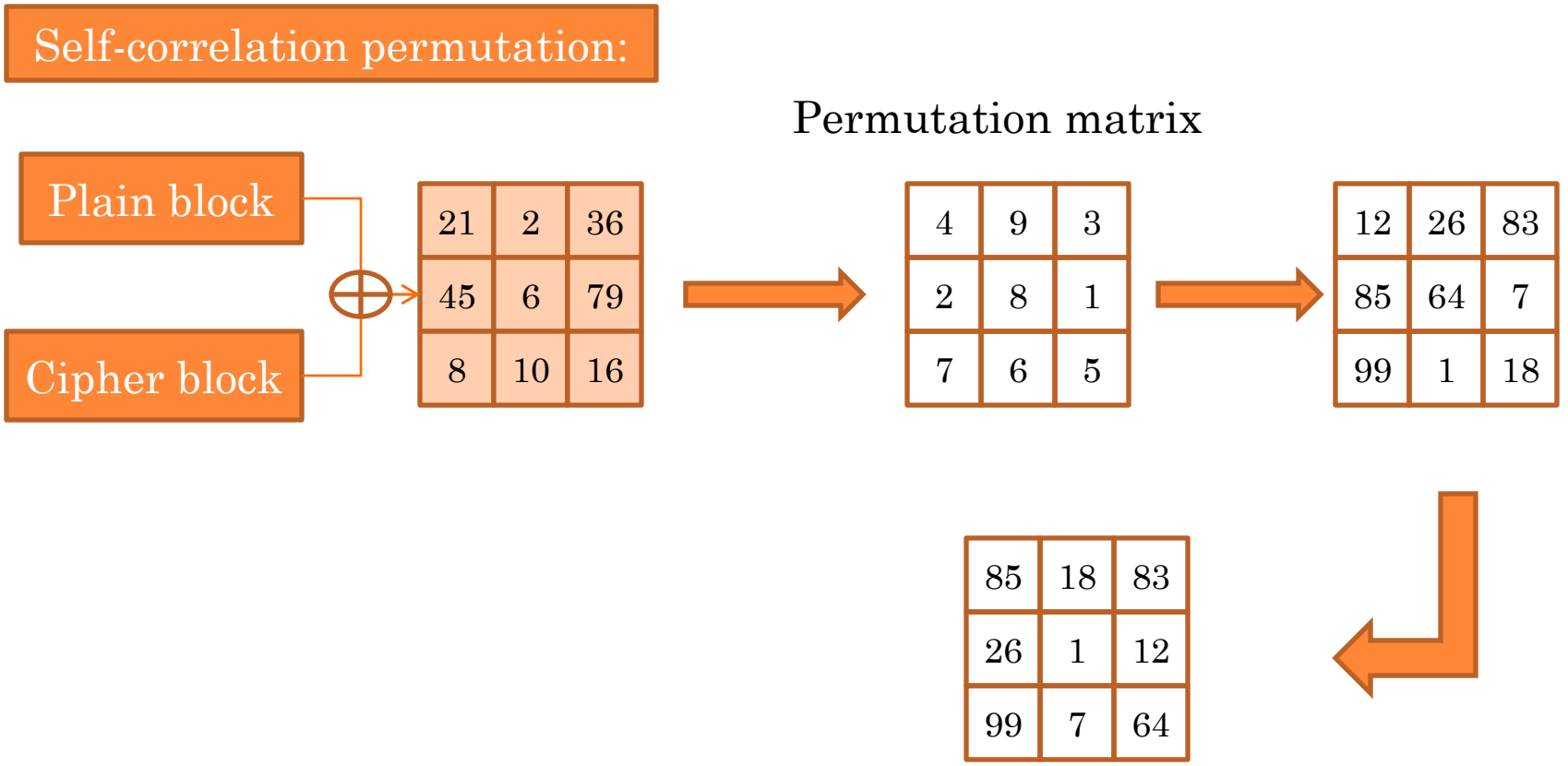
zhaoliang@itslab.csce.kyushu-u.ac.jp

IMAGE ENCRYPTION BASED ON SC-PCC FRAMEWORK



zhaoliang@itslab.csce.kyushu-u.ac.jp

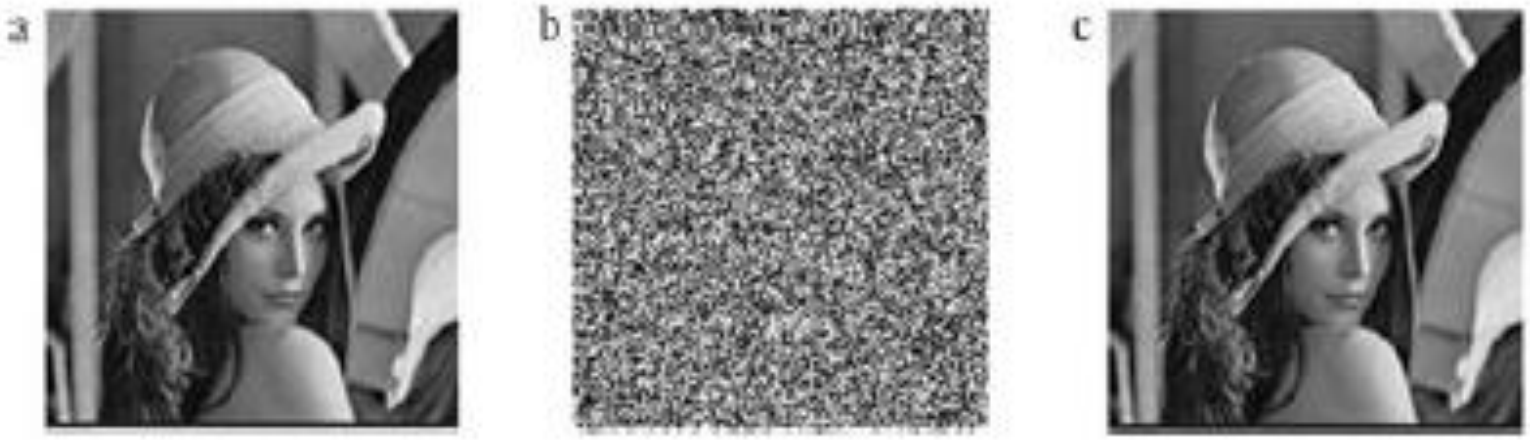
Image Encryption Based on SC-PCC Framework



zhaoliang@itslab.csce.kyushu-u.ac.jp

Image Encryption Based on SC-PCC Framework

- Simulation result:



zhaoliang@itslab.csce.kyushu-u.ac.jp

IMAGE ENCRYPTION BASED ON SC-PCC FRAMEWORK

- Test results:

Table 1: Entropy of cipher images

Test image	Size	Proposed scheme
Lena	128×128	7.9898
Baboon	128×128	7.9892
Clock	256×256	7.9144
Moon surface	256×256	7.9144
Elaine	512×512	7.9994

Table 2: Correlation coefficients of two adjacent pixels in plain image and corresponding cipher image

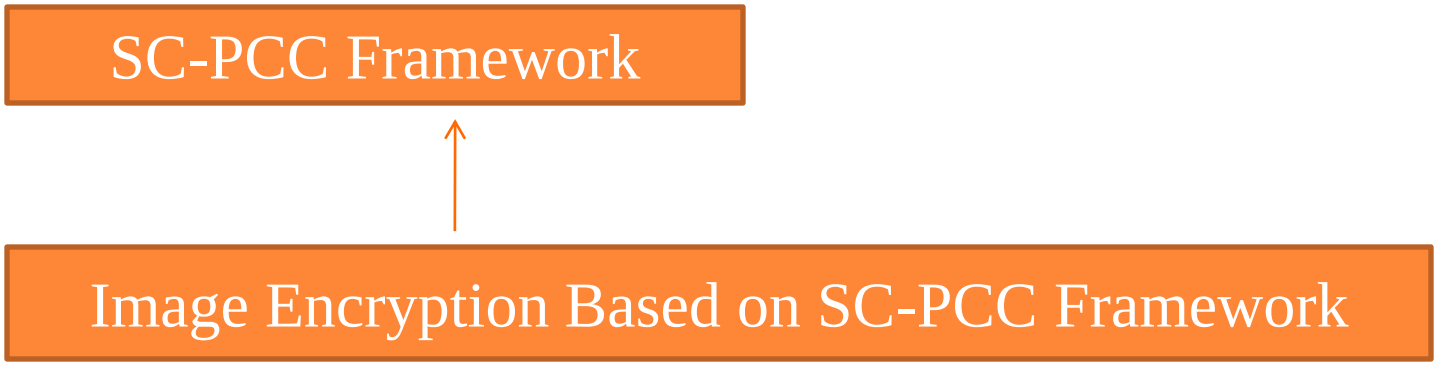
	Plain image					Cipher image				
	Lena	Baboon	Clock	Moon surface	Elaine	Lena	Baboon	Clock	Moon surface	Elaine
Horizontal	0.9418	0.8463	0.9707	0.9364	0.9703	0.0271	0.0039	-0.0424	0.0104	0.0099
Vertical	0.8903	0.8442	0.9569	0.8996	0.9739	-0.0599	-0.0263	0.0126	-0.0229	0.0152
Diagonal	0.8352	0.7917	0.9387	0.9099	0.9672	0.0052	0.0237	0.0252	-0.0434	0.0085

Table 3: NPCR and UACI of three cipher images

	Round	1	**2**	**3**	4	5	6
Lena	NPCR	0.900940	0.993896	0.996765	0.996521	0.996765	0.995728
	UACI	0.303160	0.331353	0.336692	0.333727	0.336875	0.336091
Baboon	NPCR	0.897156	0.994324	0.995728	0.996155	0.996277	0.996582
	UACI	0.300442	0.334636	0.333658	0.336958	0.336512	0.334637
Clock	NPCR	0.943039	0.994614	0.995865	0.996231	0.996338	0.996170
	UACI	0.305384	0.336289	0.335077	0.332757	0.336658	0.335189

zhaoliang@itslab.csce.kyushu-u.ac.jp

Conclusion



zhaoliang@itslab.csce.kyushu-u.ac.jp

Thank you very much
Q&A