DCC 2021，23-26 March

Privacy-preserving Compressed Sensing For Image Simultaneous Compression-Encryption Applications

Bo Zhang*, Di Xiao+, Mengdi Wang+, and Jia Liang+

*Army Engineering University, + Chongqing University

Bo Zhang(张波)

Army Engineering University

Outline

Main contents

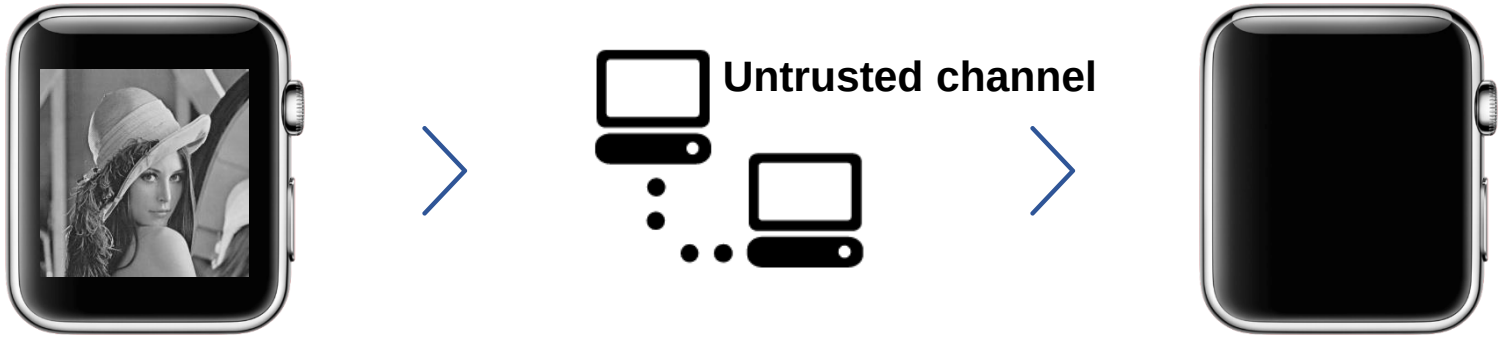
01 Background

02 Traditional CS-based cryptosystem

03 The proposed method

04 Conclusions

- Part 1 **Background Story**



Alice Charlie Bob

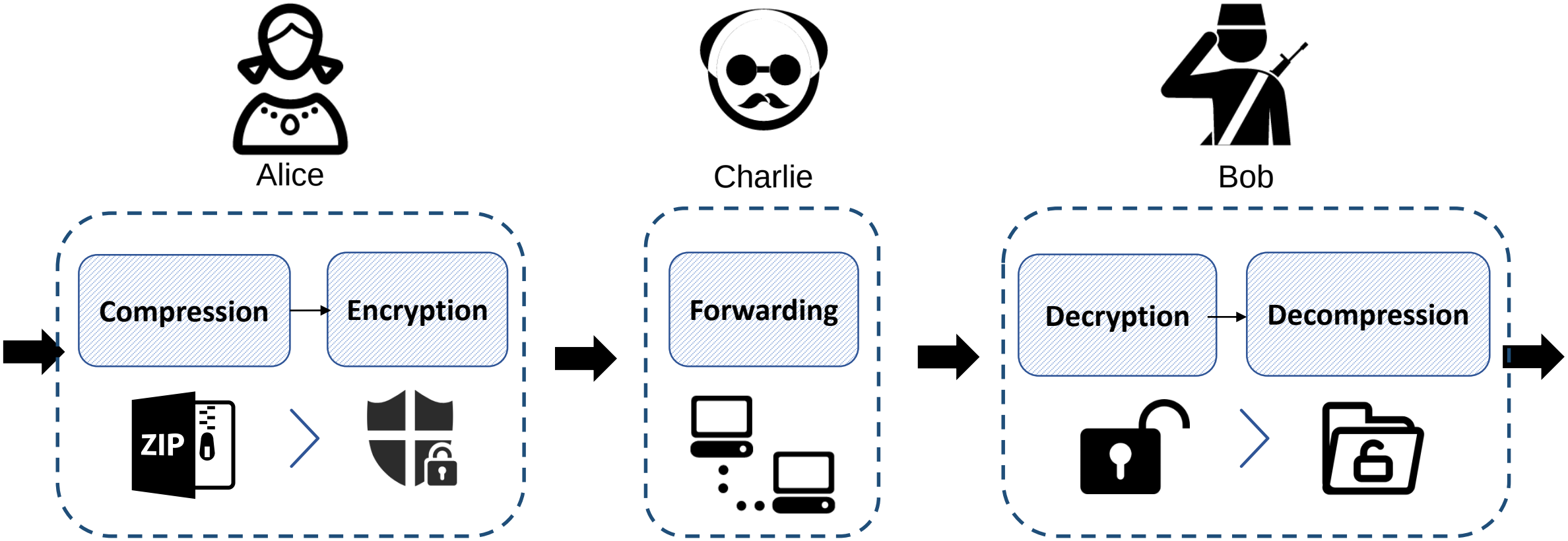
content owner → **Untrusted channel provided by Charlie.** → recipient

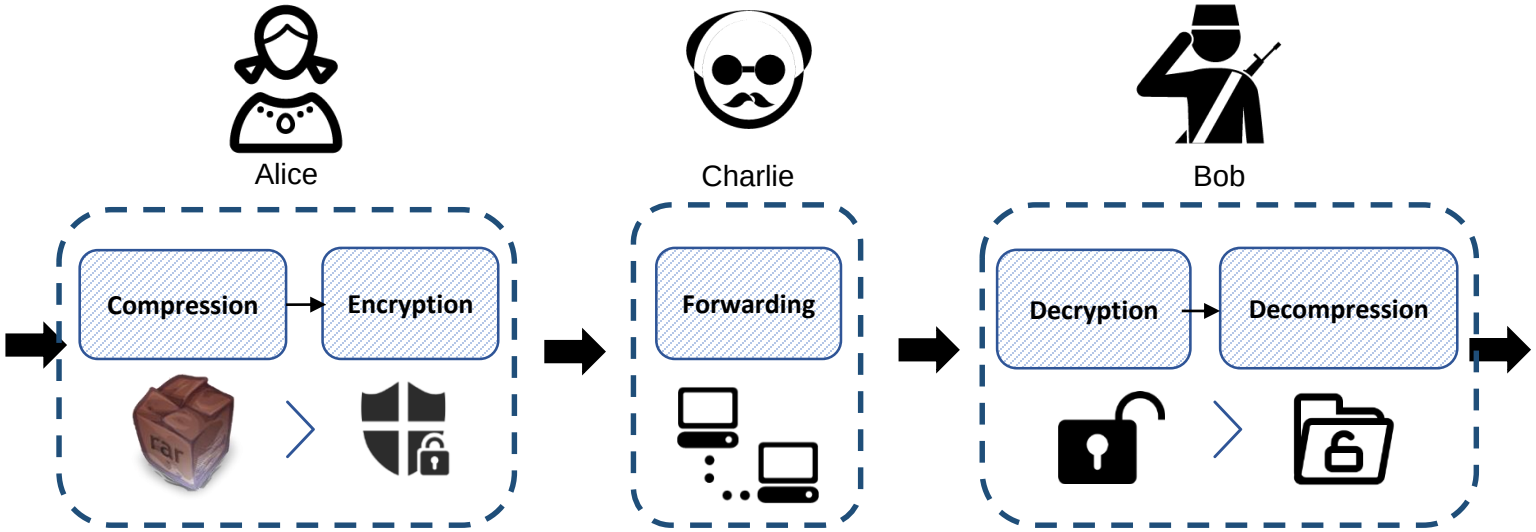
Question:

Can Alice transmit an image via untrusted channel securely and efficiently?

If she can, How?

- **Traditional** Compression-then-Encryption system





Efficient purpose

Compress the image to save channel resource.

Security purpose

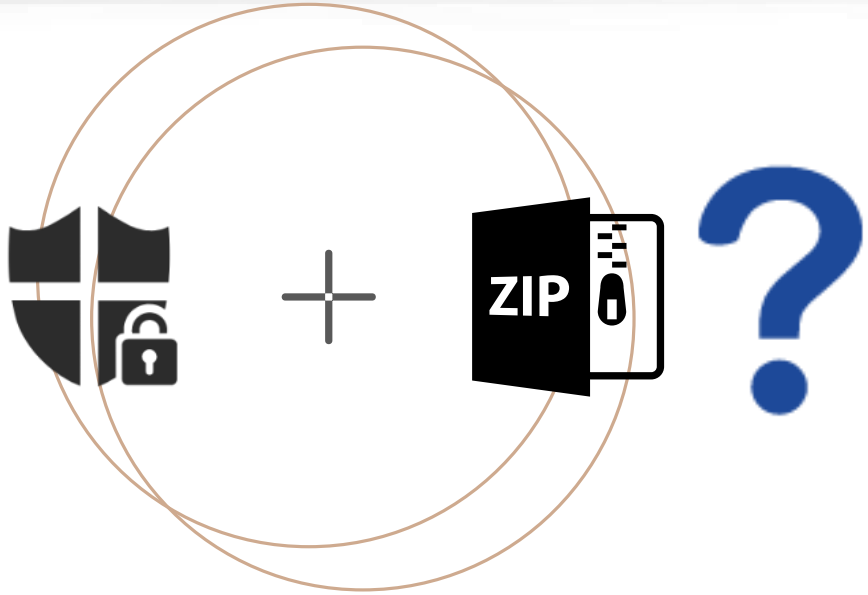
Encrypt the compressed image to mask its content.

Alice

However, in some particular scenarios, Alice uses a resource-constrained mobile device. In order to save the limited computing resources, she wants to **compress and encrypt the image at the same time**.

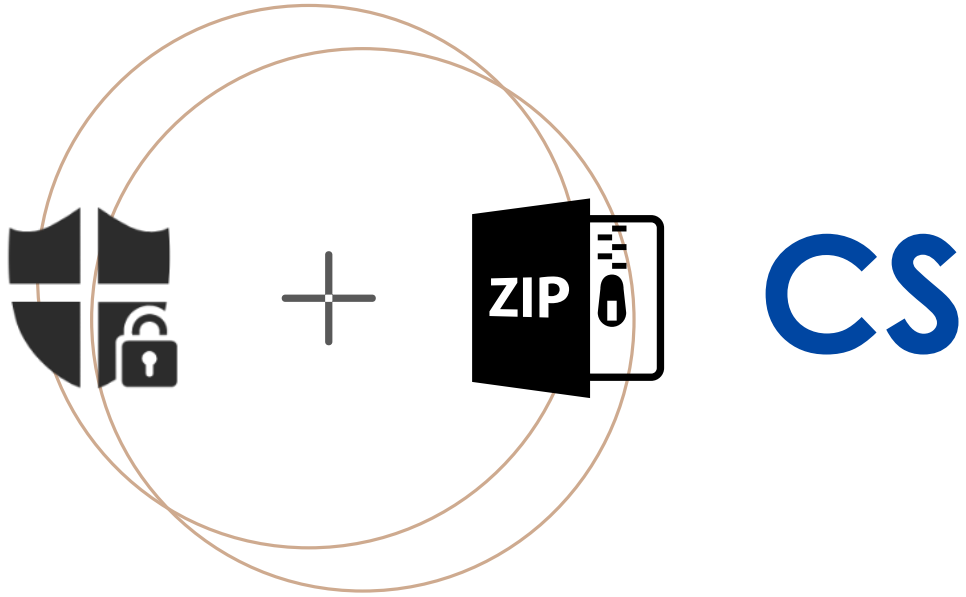
There is a question:

can Alice perform **compression and encryption at the same time**? If can, How?



Yes! She can!

Compression and encryption can be performed at the same time by using **compressed sensing (CS).**



Part 2 Traditional CS-based cryptosystem

$$y = Ax$$

$y \in R^M$

The measurement vector.

$A \in R^{M \times N} (M \ll N)$

The secret measurement matrix

$x \in R^N$

The original signal

Compression can be done by using **CS**.

Encryption also can be done by using **CS**.

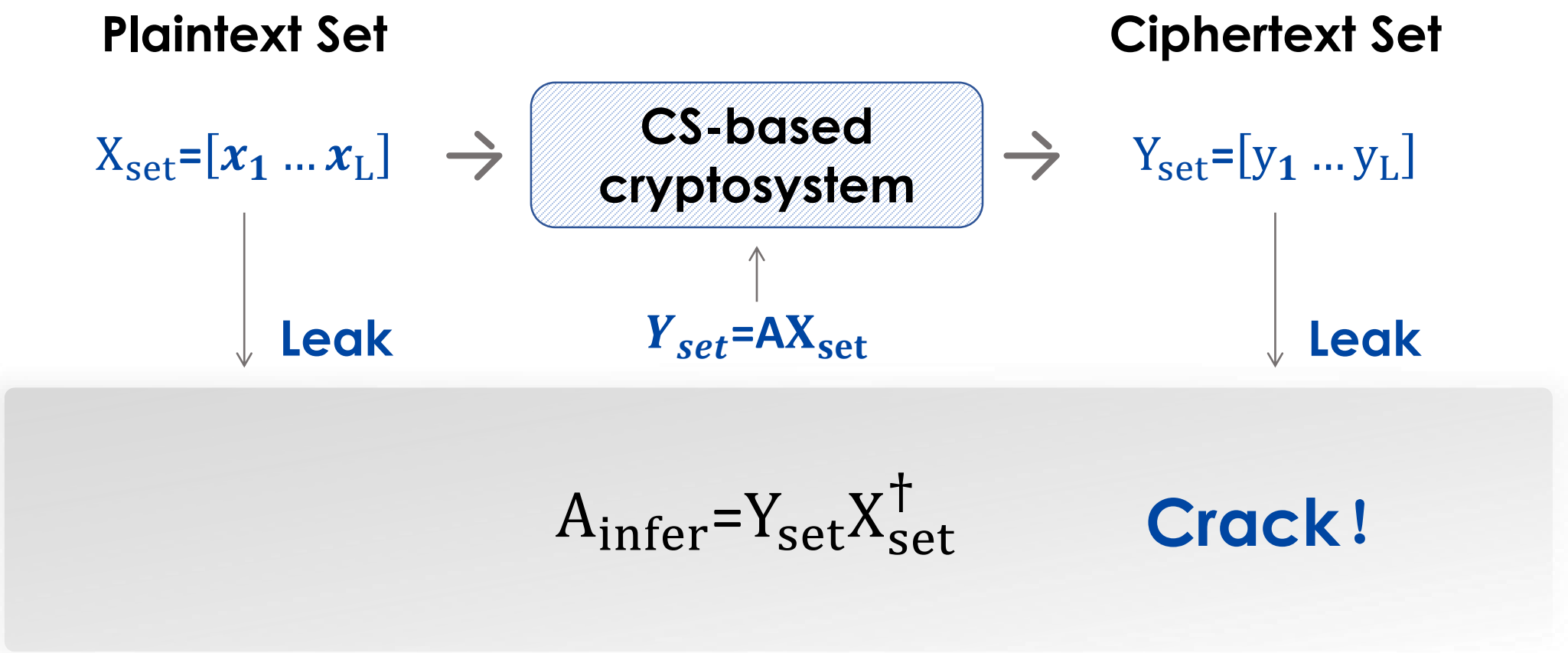
In summary, image compression and encryption can be performed at the same time by using compressed sensing.

$$y = Ax$$

However, this system cannot resist known-plaintext attack (KPA) under multi-time-sampling (MTS) scenario due to the **linearity feature of CS**.

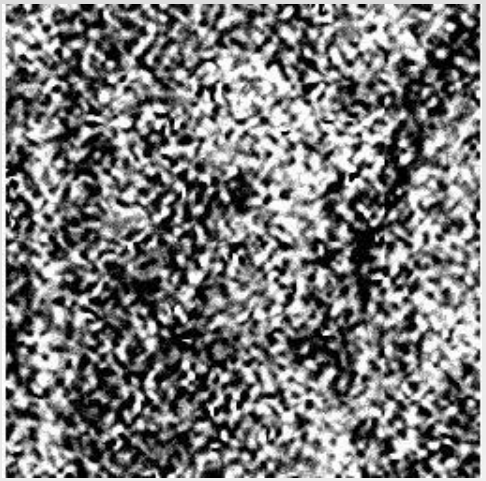
MTS scenario means that the measurement matrix is re-used a lot of times.

Known-Plaintext Attack

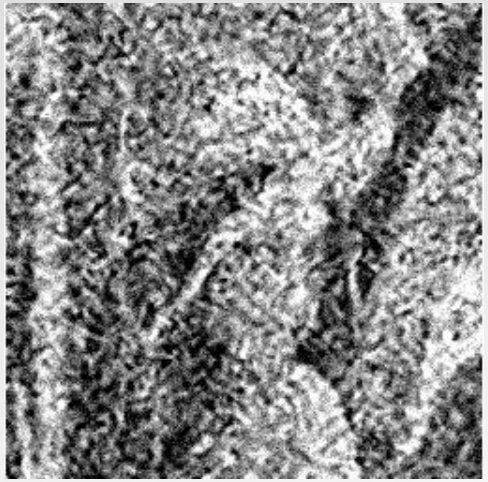


KPA simulation results

L=50



L=100



L=200

L=500

The reconstructed Lena image by using **KPA**

There is a question:

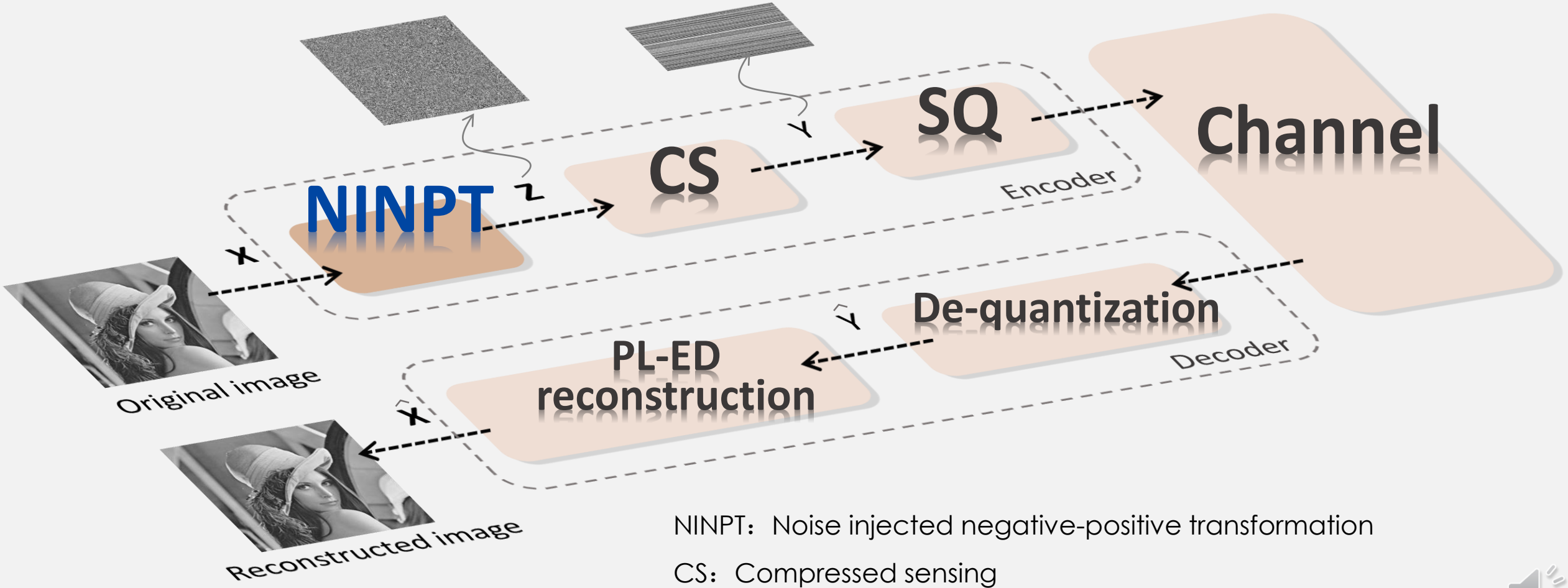
How to enhance the security of this system?

According to the above discussion,
the CS-based cryptosystem cannot resist KPA.
The reason for this is due to the linearity of its encoding process.

A solution to achieve KPA-security for this system is to break its linearity **by embedding some non-linear operations in the CS encoding process**.

- Part3 **The proposed method**

3.1 Overview



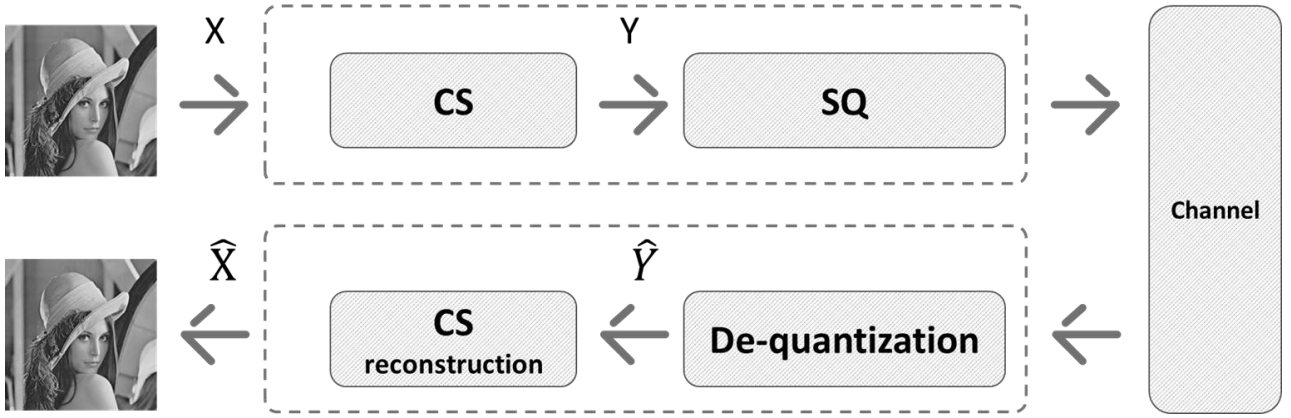
NINPT：Noise injected negative-positive transformation

CS：Compressed sensing

SQ: Scalar quantization

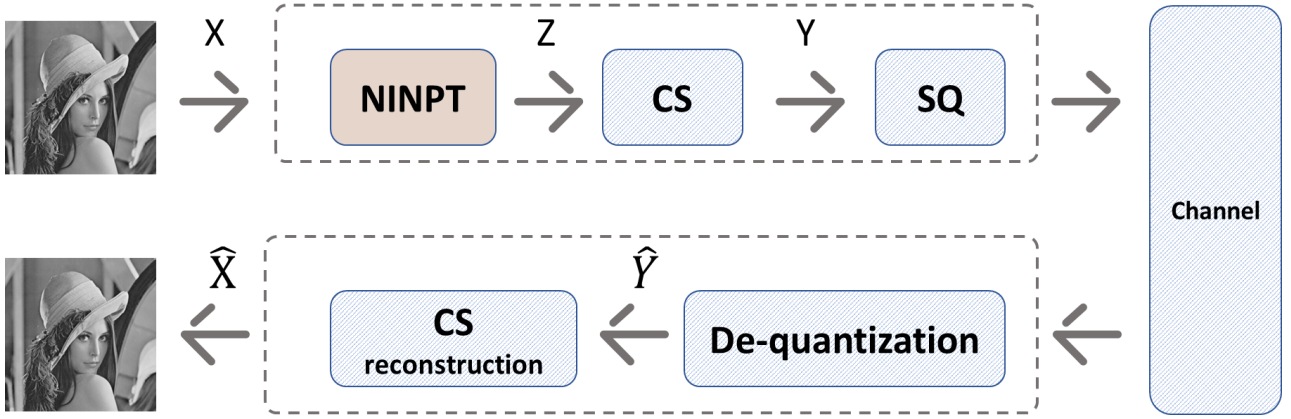
PL-ED: projected Landweber with embedding decryption algorithm

Compared with the traditional CS, the difference of the proposed method is that we embed a NINPT operation prior to CS encoding.



The traditional CS-based cryptosystem

Since the introduction of NINPT operation breaks the linearity of the CS sampling process, the proposed method can resist KPA.



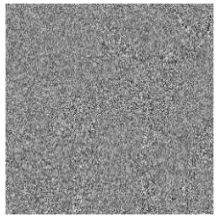
The proposed CS-based cryptosystem

3.2 Encoding steps

Step 1: Image encryption by using NINPT.

Original image

X → NINPT → Z



The intermediate ciphertext

$$Z = \mathrm{E}(X)$$

$Z \in R^{N\times N}$ The intermediate ciphertext

$\mathrm{E}(\bullet)$ The NINPT operation.

$$Z(i,j) = \begin{cases} \frac{1}{2}M(i,j) + \frac{1}{2}X(i,j), & R(i,j) = 0 \\ 255 - \left(\frac{1}{2}M(i,j) + \frac{1}{2}X(i,j),\right), & R(i,j) = 1 \end{cases}$$

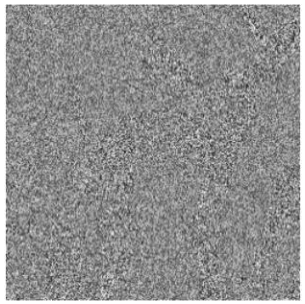
$M \in R^{N\times N}$ Pseudo-random matrix

$R \in R^{N\times N}$ Random binary integer matrix

I say NINPT operation is a non-linear operation because the ciphertext cannot be obtained by multiplying the original image by secret matrices.

3.2 Encoding steps

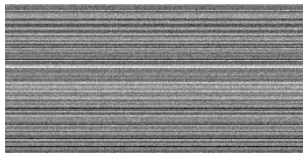
Step 2: Image compression-encryption by using CS



Z

Compressed sensing

Y



The intermediate ciphertext

The final ciphertext

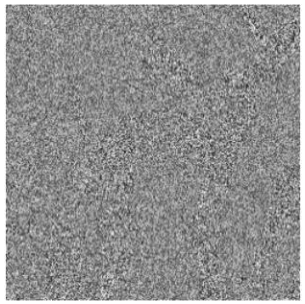
$$Y = AZ$$

$$Y \in R^{M \times N}$$

The final compressed ciphertext

3.2 Encoding steps

Step 2: Image compression-encryption by using CS

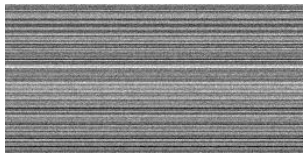


The intermediate ciphertext

Z

Compressed sensing

Y



The final ciphertext

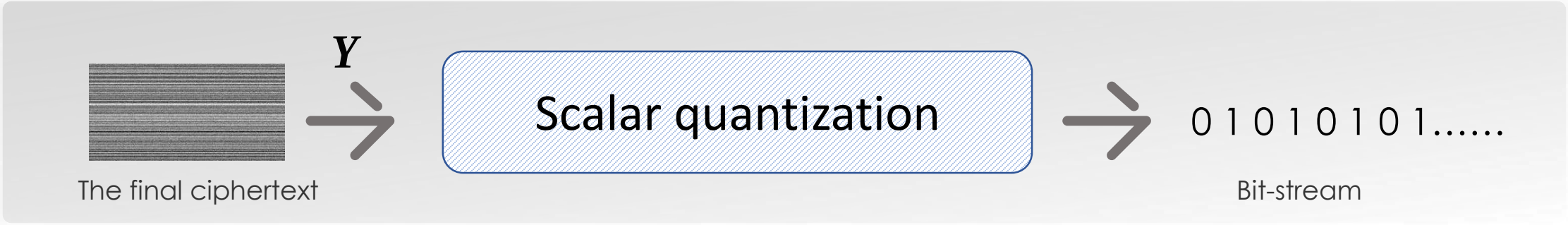
$$Y = AZ$$

Compression can be done by using **CS**.
Encryption also can be done by using **CS**.

In summary, The intermediate ciphertext is
compressed and re-encrypted by CS at the same time.

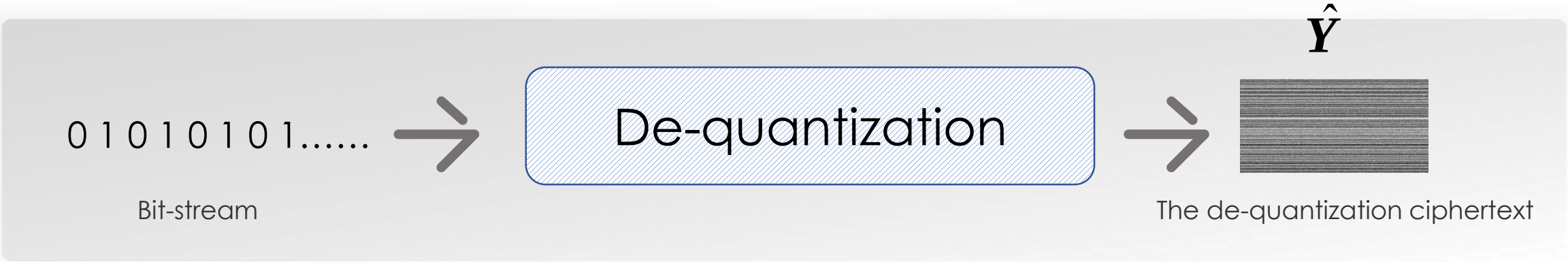
3.2 Encoding steps

Step 3: Scalar quantization.



3.3 Decoding steps

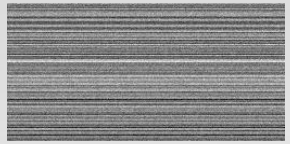
Step 1: De-quantization operation.



3.3 Decoding steps

Step 2: Image reconstruction.

$\hat{Y}$



The de-quantization ciphertext

Image reconstruction

$\hat{X}$

Reconstructed image

A big challenge is encountered:

how can we recover the original image effectively.

3.3 Decoding steps

Step 2: Image reconstruction.

By taking the encryption into consideration,
the joint image reconstruction can be achieved by using this equation

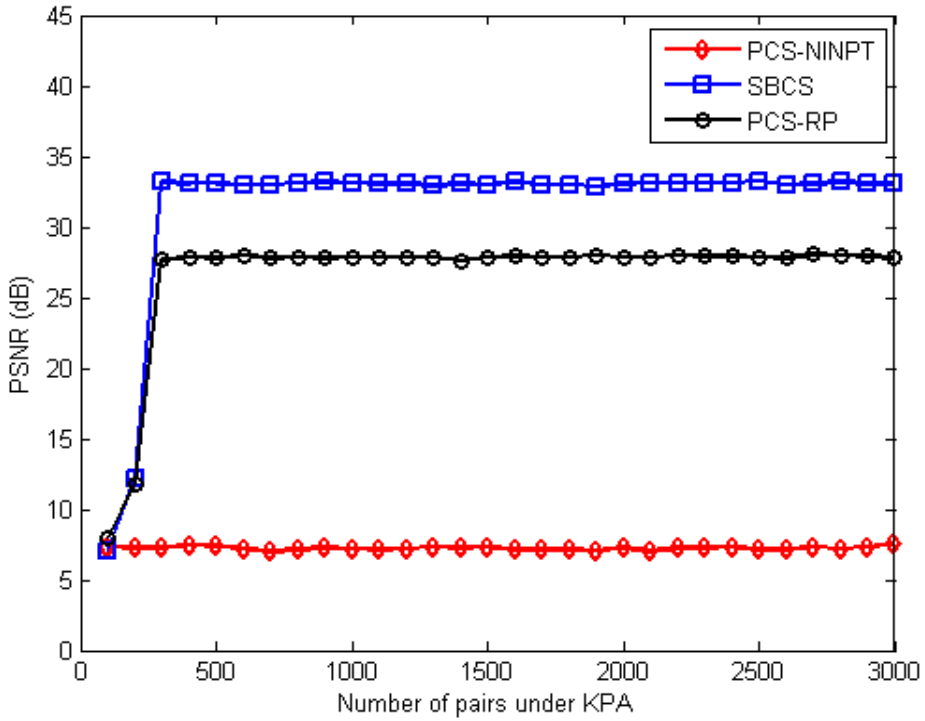
$$\hat{\boldsymbol{X}} = \arg\min_{\boldsymbol{X}} f(\boldsymbol{X}) = \frac{1}{2}\left\|\hat{\boldsymbol{Y}} - \boldsymbol{\Phi}\,\mathrm{E}(\boldsymbol{X})\right\|_F^2 + \beta\left\|\boldsymbol{\Psi}\boldsymbol{X}\boldsymbol{\Psi}^{\mathrm{T}}\right\|_1$$

$\boldsymbol{\Psi} \in R^{N\times N}$
a wavelet basis matrix

A projected Landweber with embedding decryption (PL-ED) algorithm is proposed,
where the image is recovered in an iterative manner.

3.4 Simulations results

Security performance evaluation



Average PSNR under KPA for Lena image (256×256).

3.4 Simulations results

Compression performance evaluation

Images	Schemes	Bit rates					
		0.5	1.0	1.5	2.0	2.5	3.0
Lena	**PCS-CME**	11.22	20.02	25.07	25.93	28.05	29.13
	PCS-RP	18.16	22.68	26.28	27.89	29.92	32.44
	SBCS	24.91	29.72	31.78	33.36	34.87	36.19
	PCS-NINPT	24.22	28.93	30.66	31.99	33.47	34.64

Therefore, we can conclude that the proposed cryptosystem can resist KPA at the cost of slightly sacrificing the compression performance.

- Part4 **Conclusions**

4.1 Conclusion

In this paper,
a novel privacy-preserving CS scheme for image
simultaneous compression-encryption applications is proposed.

4.1 Conclusion

In summary, the contributions of this paper are as follows:

- **The introduction of NINPT operation in the CS encoding process breaks the linearity of the CS sampling process, which makes the proposed method can withstand KPA. To the best of our knowledge, it is the first time a non-linear operation is embedded in the CS encoding process to withstand KPA.**

- **A PL-ED algorithm is proposed, which can be used to reconstruct the image effectively even if the intermediate ciphertext is not sparse anymore.**

Thank you !