ICASSP'18 Calgary, Alberta, Canada

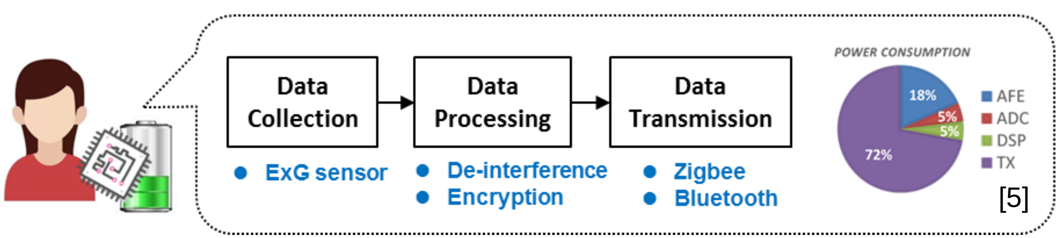
Low-complexity Secure Watermark Encryption for Compressed Sensing-based Privacy Preserving

Speaker: Ting-Sheng Chen
Advisor: Prof. An-Yeu (Andy) Wu
Institute: National Taiwan University
Date: 2018/04/20

Wireless Sensor Networks (WSN) in IoT

WSN is key element of IoT

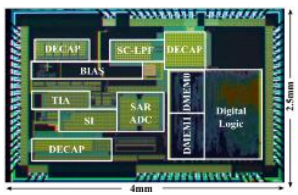
- Wireless Sensor Network (WSN) [1-2]
  - Acquire large amounts of data locally
  - Extremely tight resource budgets
- Implementation issues of WSN [3-4]
  - Limited bandwidth & complexity →***Data compression***
  - Privacy Leakage → ***Data Encryption***



Compressed Sensing (CS) : Enable reduced-complexity of sensor with data hiding

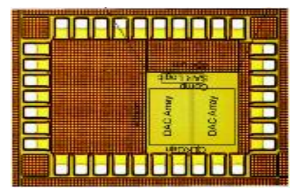
Promising Technique in WSN: Compressed Sensing (CS)

- CS front-end sensor
  - Reduce data rate & complexity



ISSCC, 2016 [8]

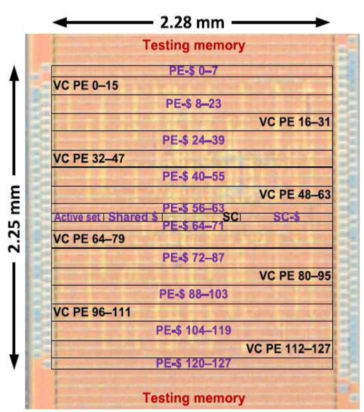
Application: PPG



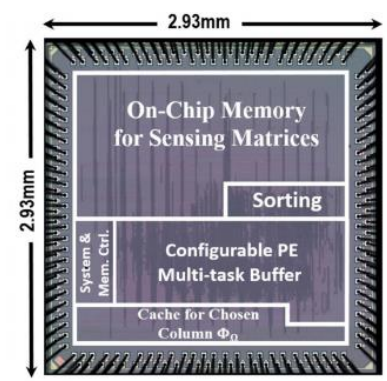
JSSC, 2017 [9]

Application: Speech Signal

- CS back-end solver
  - Reconstruct signal from low to high-dimension

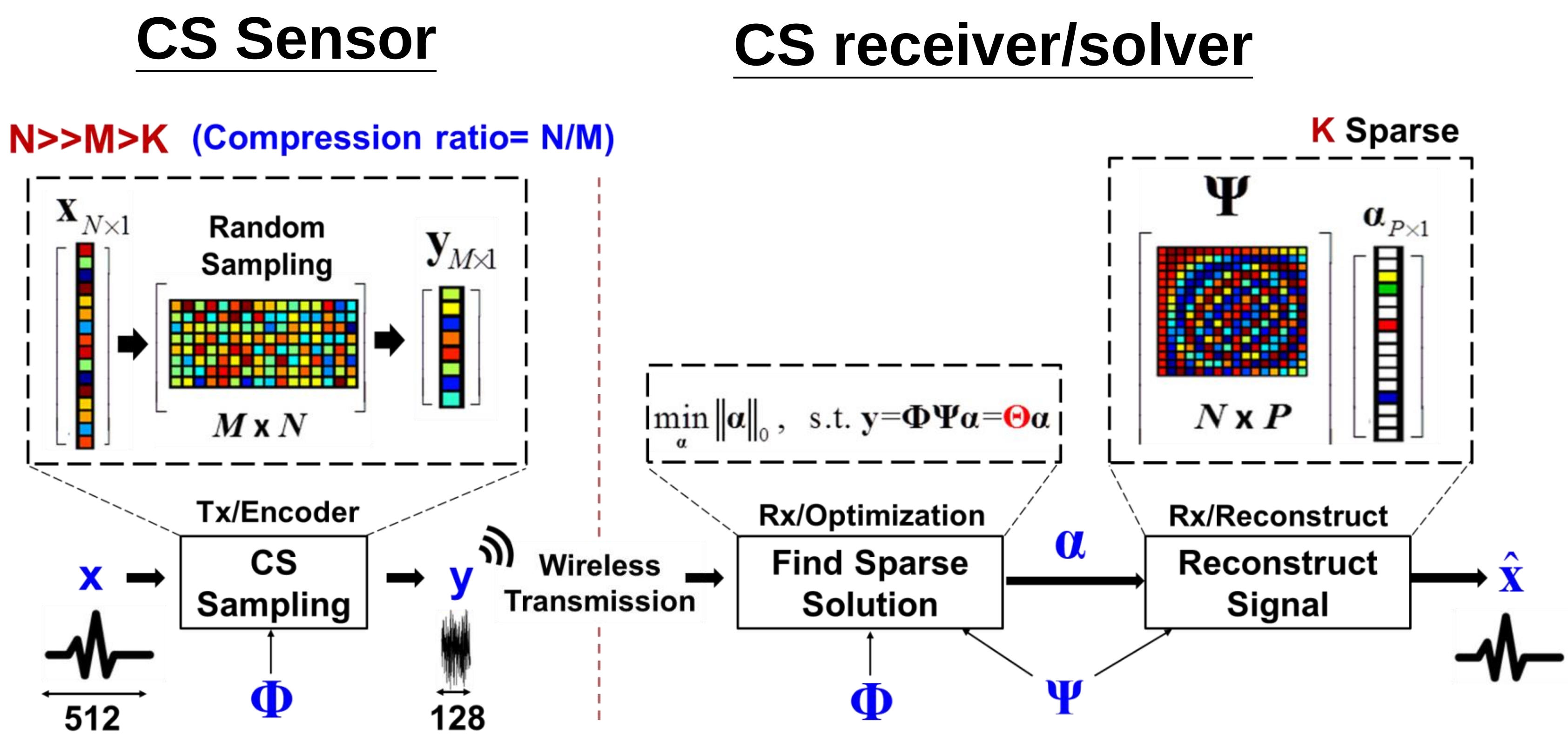


ISSCC, 2015 [10]



ISSCC, 2018 [11]

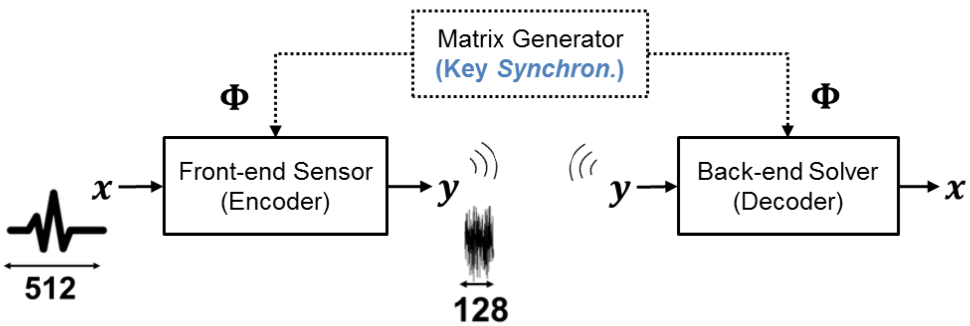
Framework of Compressed Sensing [8-9]



- Achieve ***N/M Compression Ratio (CR)*** through **random sampling**
- Move the data acquisition overheads to receiver

Compressed Sensing w/ Inherent Encryption

- ***y*** can not be reconstructed successfully w/o explicit $\boldsymbol{\Phi}$ [12-15]
  - CS can be regarded as a private key cryptosystem



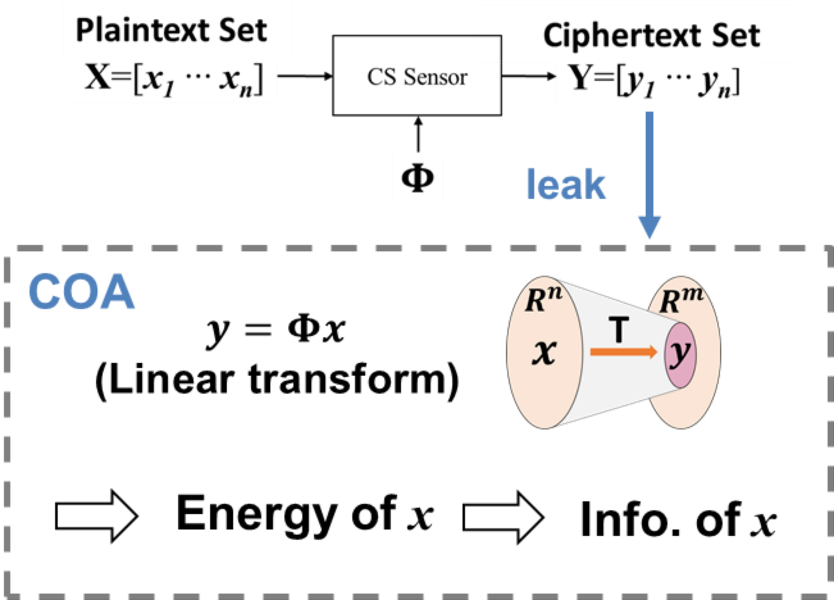
Secure Model	CS model
Plaintext	Sensed Data ($\boldsymbol{x}$)
Ciphertext	Transmitted data ($\boldsymbol{y}$)
Private Key	Sensing matrix ($\boldsymbol{\Phi}$)

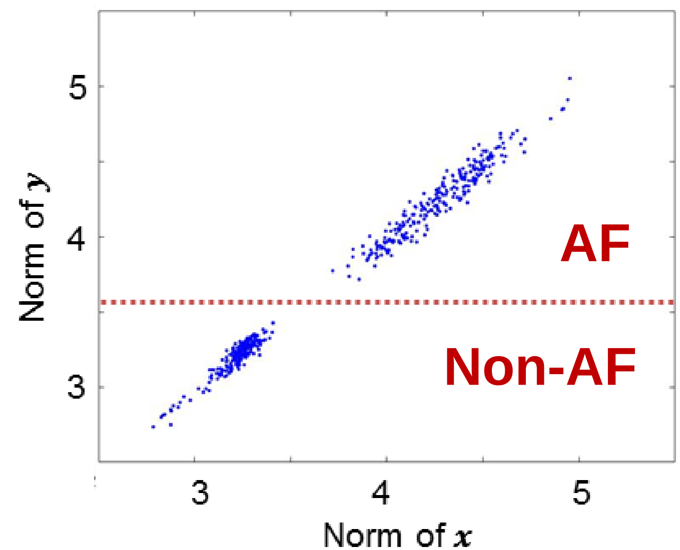
- Information leakage due to linearity of CS encoding process
  - Ciphertext-Only Attack (COA) [16]
    → Eve crack ciphertext (***y***)
  - Known-Plaintext Attack (KPA) [17]
    → Eve crack plaintext - ciphertext (***x***, ***y***)

Compressed Sensing under Ciphertext-Only Attack (COA) [16]

- *y* (ciphertext) are leaked
- Target info. → Info. of *x*

- For example
  - Energy of y is able to classify **Atrial Fibrillation** (AF) or non-AF





Secure Goal against COA: *y* won't reveal info. of ***x***

Compressed Sensing under Known-Plaintext Attack (KPA) [17]

- ($\boldsymbol{x}$, $\boldsymbol{y}$) pair are leaked
- Target info. → $\boldsymbol{\Phi}$

Plaintext Set $X=[x_1 \cdots x_n]$ → CS Sensor → Ciphertext Set $Y=[y_1 \cdots y_n]$

$\boldsymbol{\Phi}$ → CS Sensor

leak

leak

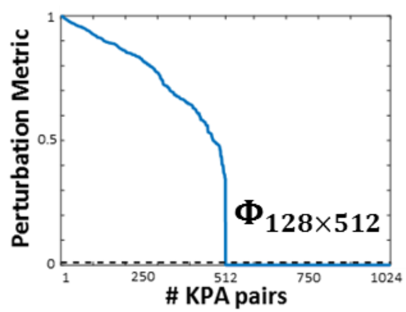
Only y leak

KPA

$$Y = \Phi_{EVE} X$$

⇩

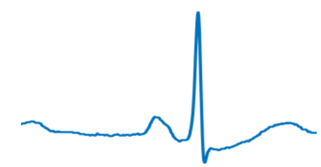
$$\Phi_{EVE} = Y X^{\dagger}$$



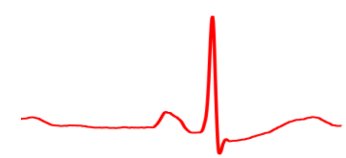
⇨

After 10 mins

Plaintext



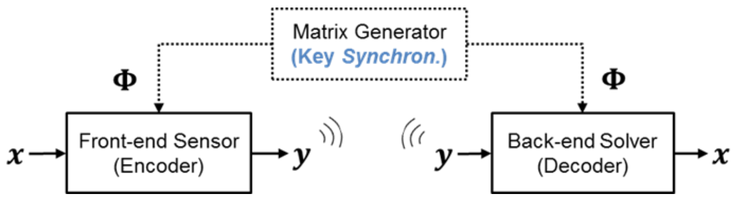
Cracked by KPA



Secure Goal against KPA: Increasing pairs of ($\boldsymbol{x}$, $\boldsymbol{y}$) to crack $\boldsymbol{\Phi}$

Prior Art : Multiple Sensing Matrices [18-21]

- Φ is acted as a shared secret key



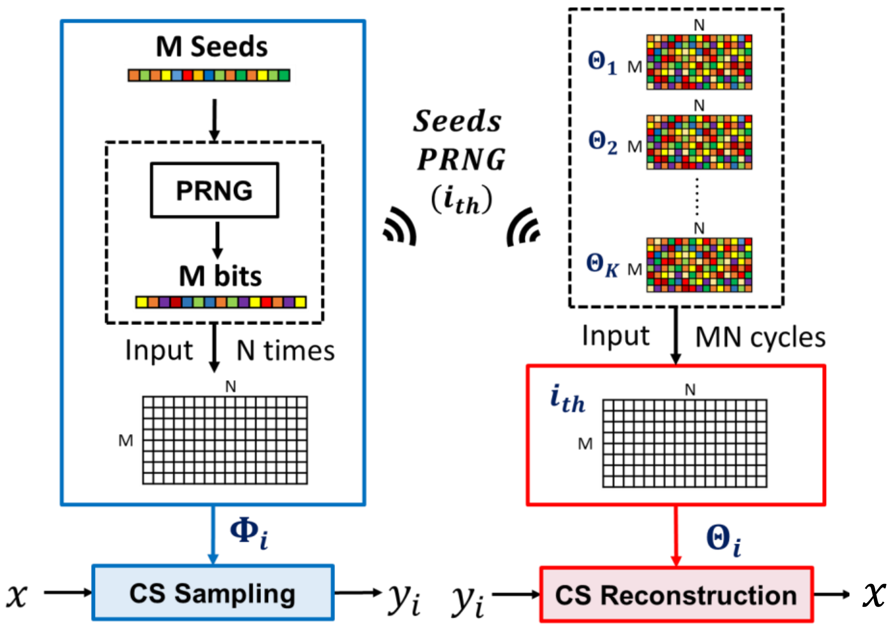
Utilize multiple Φ to enhance security level

- Challenge of multiple Φ
  - High complexity of front-end sensor

Not suitable for the demand of IoT applications

  - Synchronization issue

Security level increases only linearly as # Φ increases



Design Goal of CS-based Privacy Preserving for WSN in IoT

- Prevent from **privacy leakage**
  - Cope with ***Ciphertext-Only Attack (COA)***

    Make y unable to leak explicit information of x

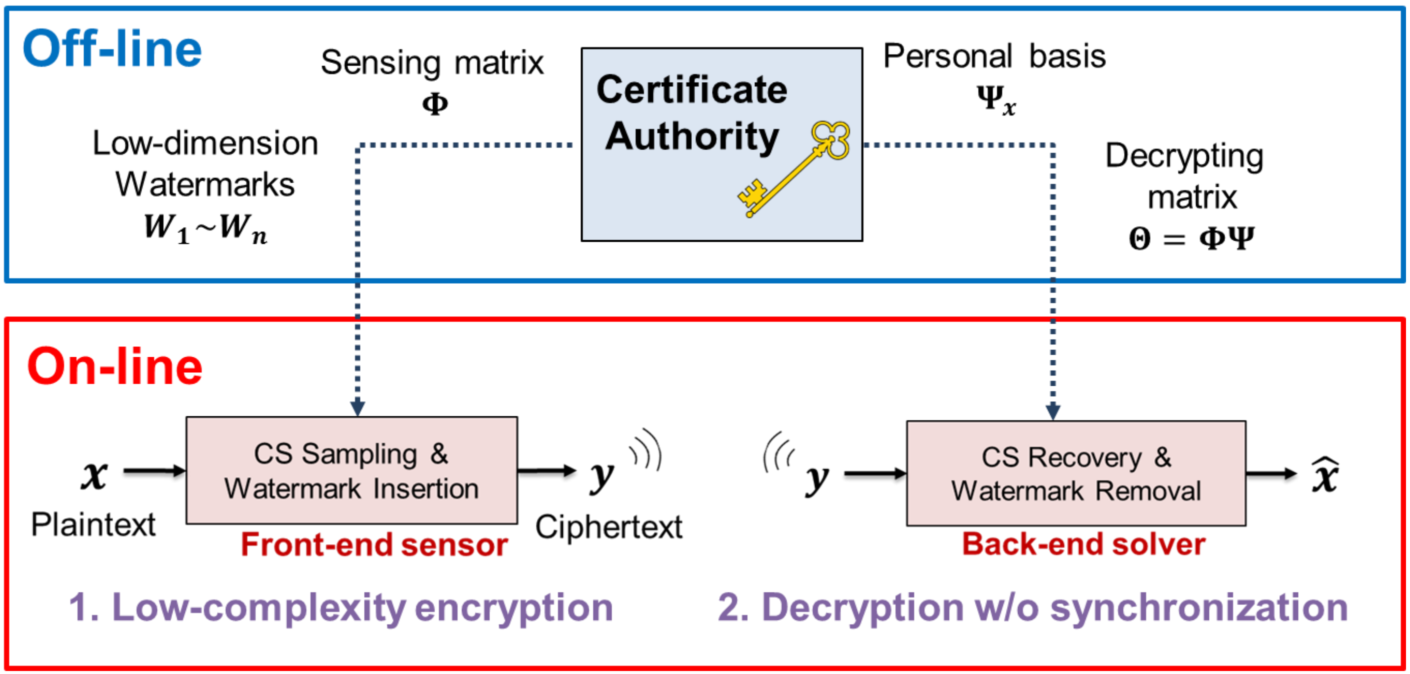
  - Cope with ***Known-Plaintext Attack (KPA)***

    Increase # collected **(x, y)** for recoverable estimation performed by Eve

- Suit for **Realistic IoT application**
  - **Low overhead** in *Front-end Sensor*
  - **Free from *Synchronization***

Proposed CS-based Privacy Preserving: Overview

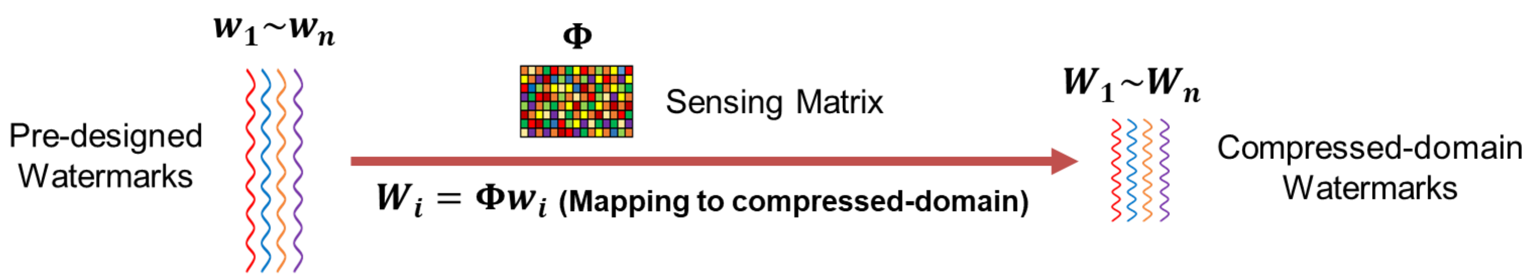
- Proposed encoding equation: $y = \Phi x + W_i$ (i: randomly chosen from 1 to n)
  - Leverage "cons of CS": CS is sensitive to measurement noise
- Flowchart of proposed CS-based privacy preserving



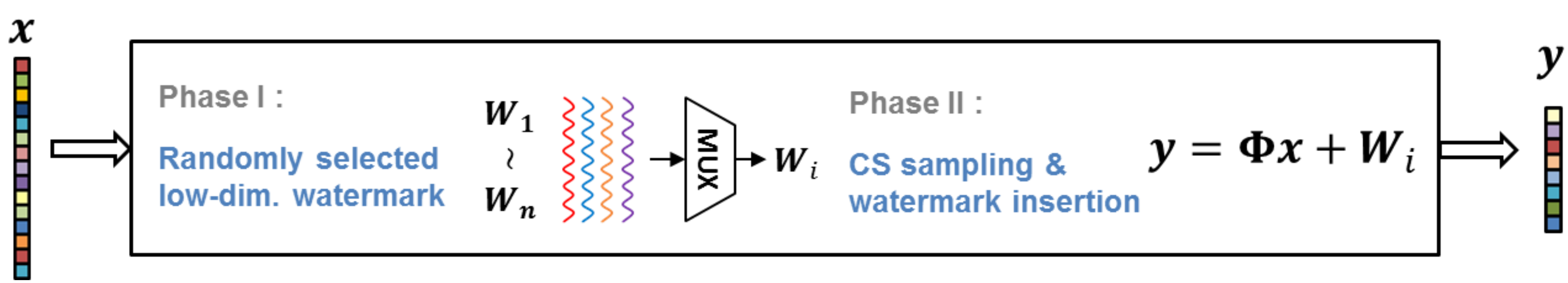
Proposed Framework: Front-end Sensor

- Multiple watermarks enhances security level
- Compressed watermarks is less complexity of storage & computation

Off-line Stage of Front-end Sensor



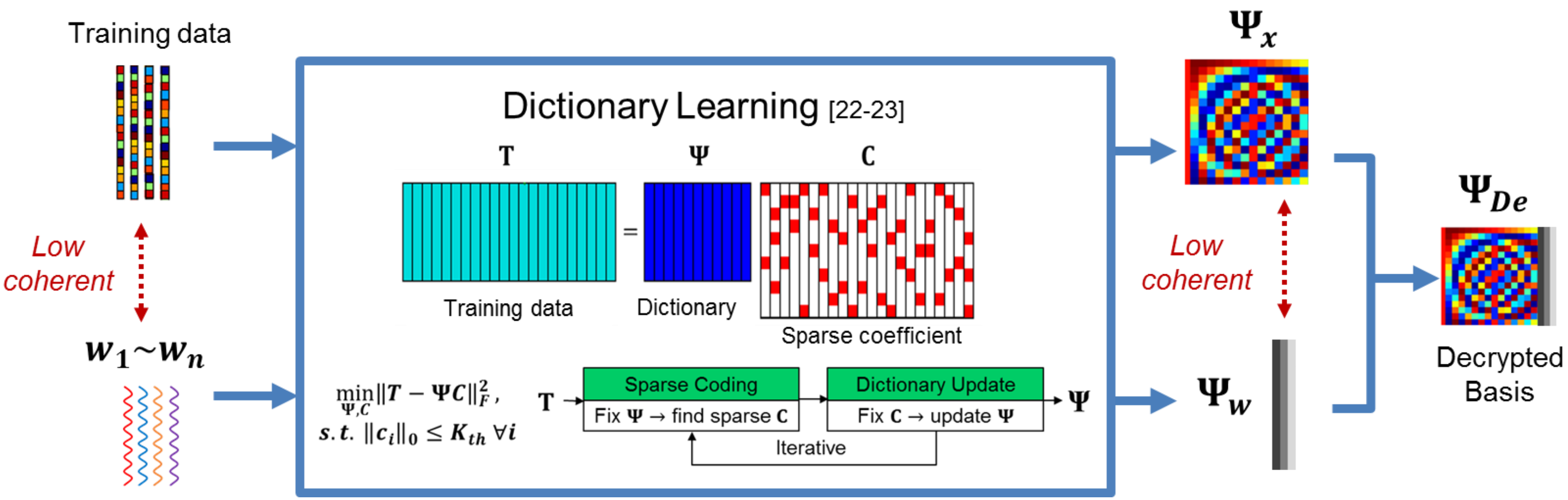
On-line Stage of Front-end Sensor



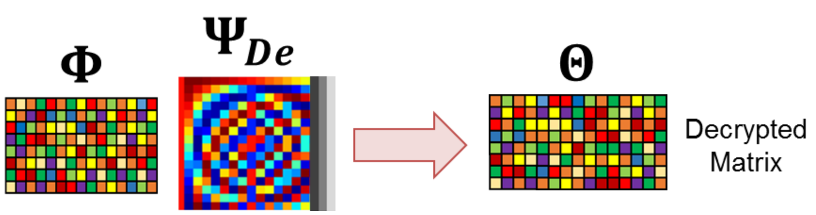
Proposed Framework: Back-end Solver (1/2)

Off-line Stage of Back-end Solver

Phase I : Decrypted basis generating



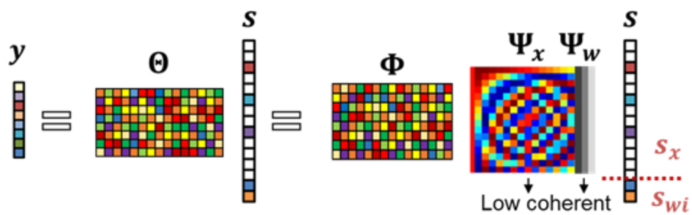
Phase II : Decrypted matrix generating



Proposed Framework: Back-end Solver (2/2)

Proposed On-line stage

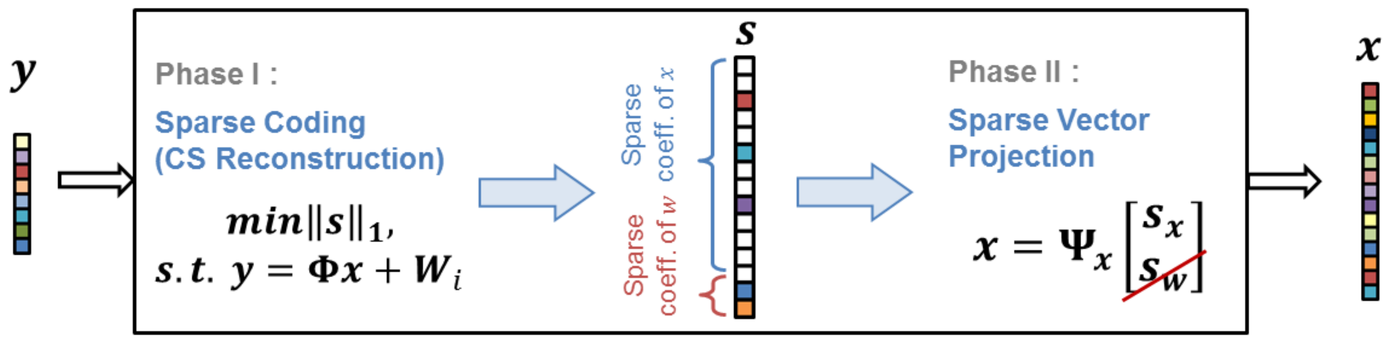
$$\min\|s\|_1, s.t.\ y = \Phi x + W_i$$



$$y = \Phi(x+w) \quad \text{CS encoding}$$
$$= \Phi\Psi_x s_x + \Psi_w s_{wi}$$
$$= \Phi[\Psi_x \Psi_w][s_x s_{wi}]^{\mathrm{T}}$$
$$= \Phi\Psi_{De} s \quad \text{CS decoding}$$

1. s can separated into two regions (Ψ_x and Ψ_w are low coherent)
2. ***Sparse vector of random selected W can be mapped to s_w***

On-line Stage of Back-end Solver



Simulation Settings

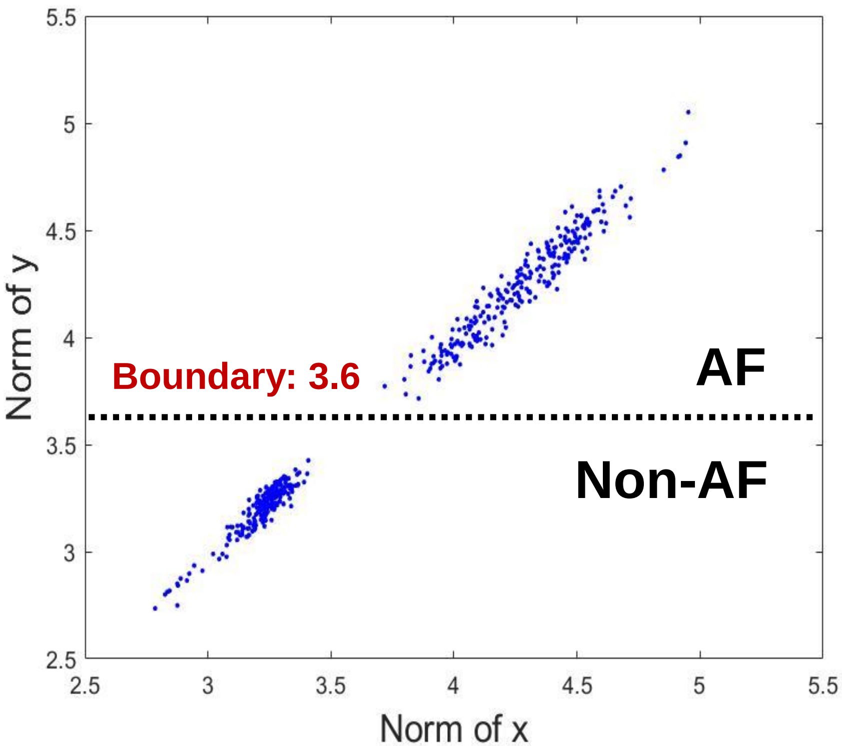
- Database
  - ECG sampled at $f_s = 512Hz$ from *National Taiwan University Hospital*

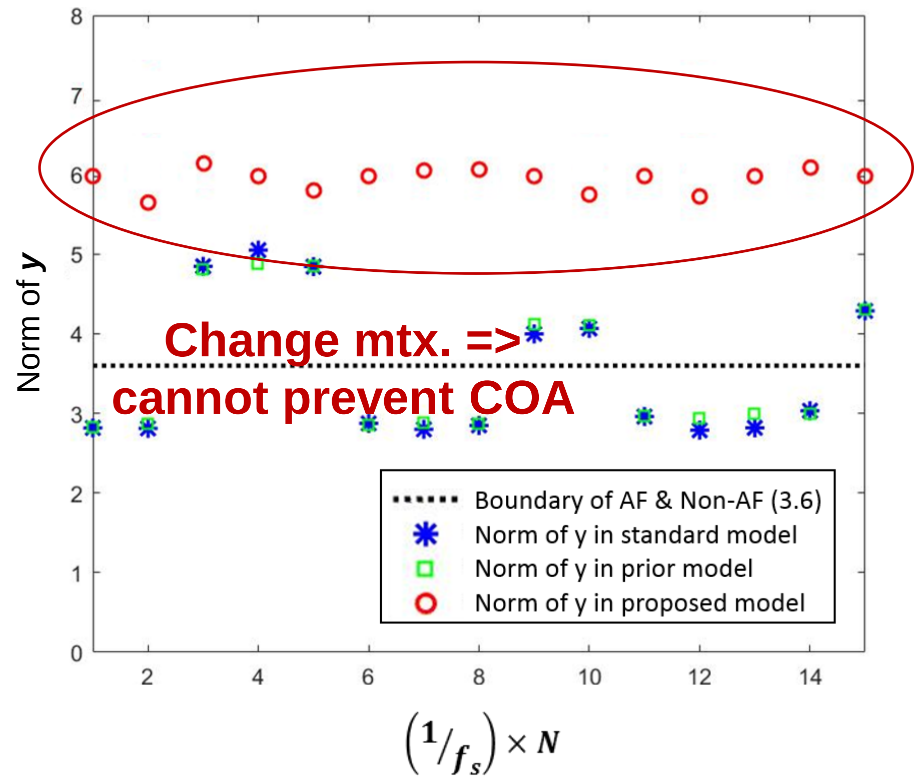
	Prior model [18-21]	**Proposed model**
Security Mechanism	Multiple sensing matrices	Multiple watermarks
Off-line Parameter Setting		
# training vectors	2500	2500
# columns of Ψ_x	512	504
# columns of Ψ_w	-	8
On-line Parameter Setting		
# testing vectors	1500	1500
Dim. of measurement (M)	128	128
# sensing matrices / watermarks	8	8

Simulation Result under Ciphertext-Only Attack (COA)

- ***y*** (ciphertext) are leaked
  - COA can estimate info. of ***x***

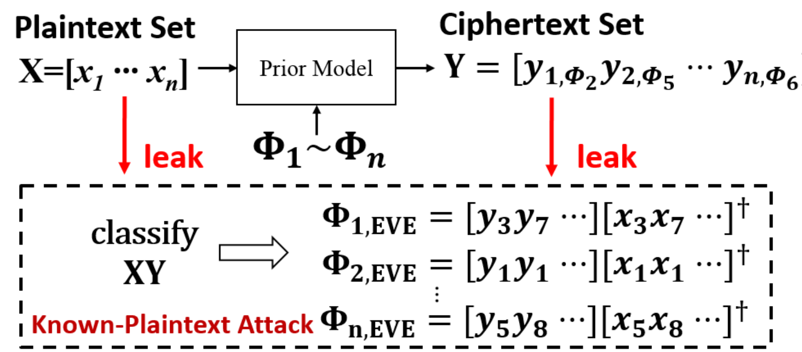
Proposed model:
Energy of measurements is disturbed



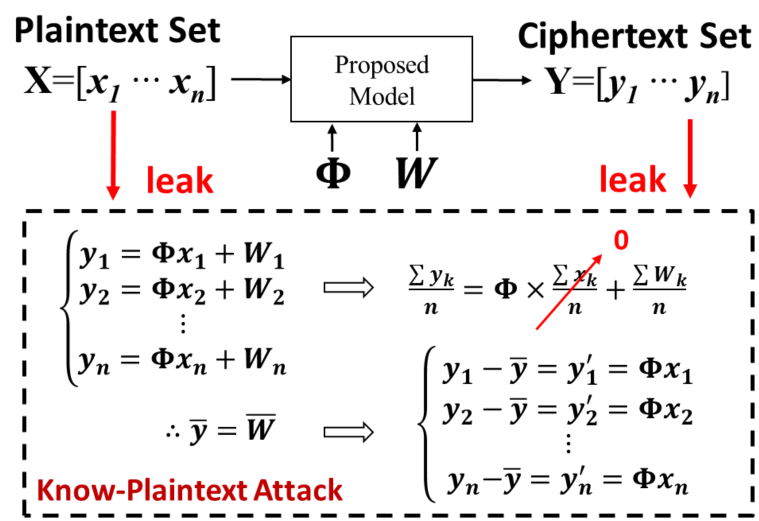


Cracking Mechanism of Known-Plaintext Attack (KPA)

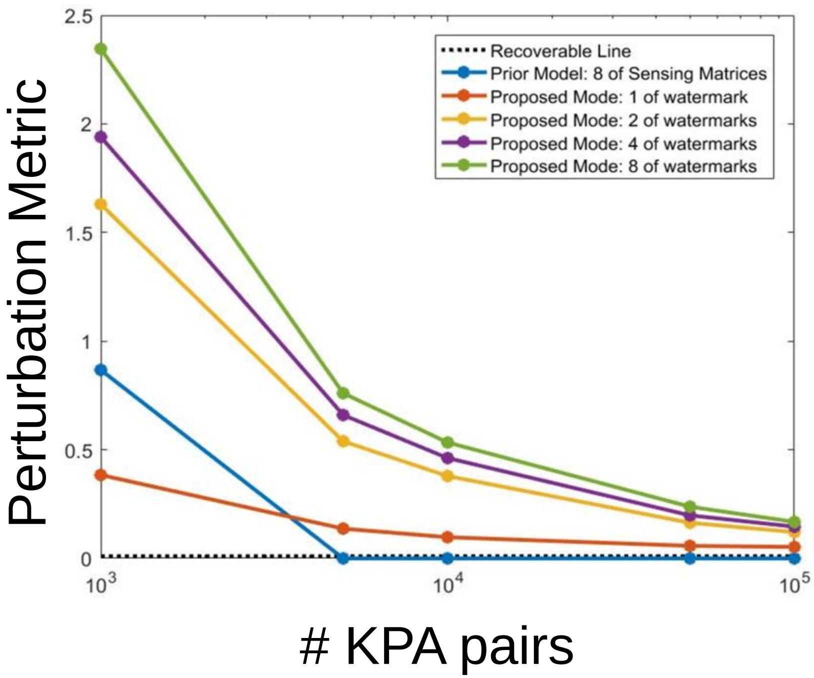
- If **(*x*, *y*)** pair are leaked
  - KPA want to estimate Φ
- KPA under prior model
  - Due to synchronization
  - Order of key are leaked

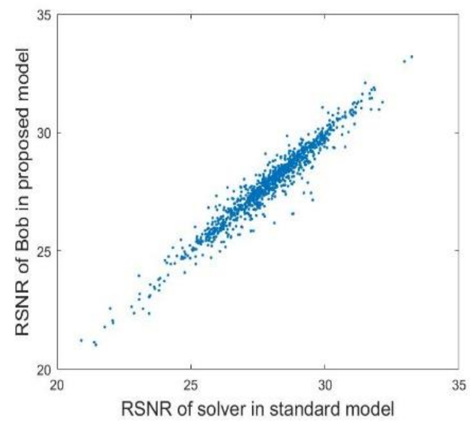


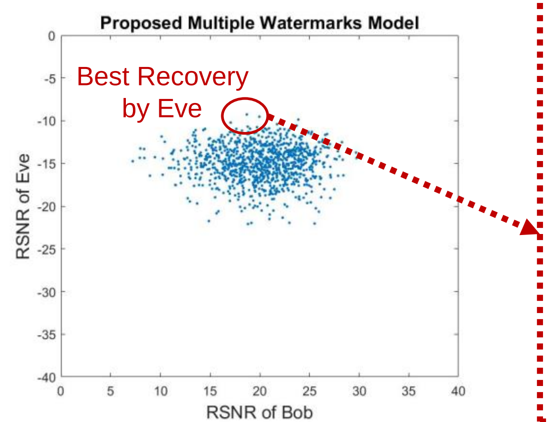
- KPA under proposed model
  - If Eve know there is some watermarks
  - Eve try to average the measurement to crack watermark

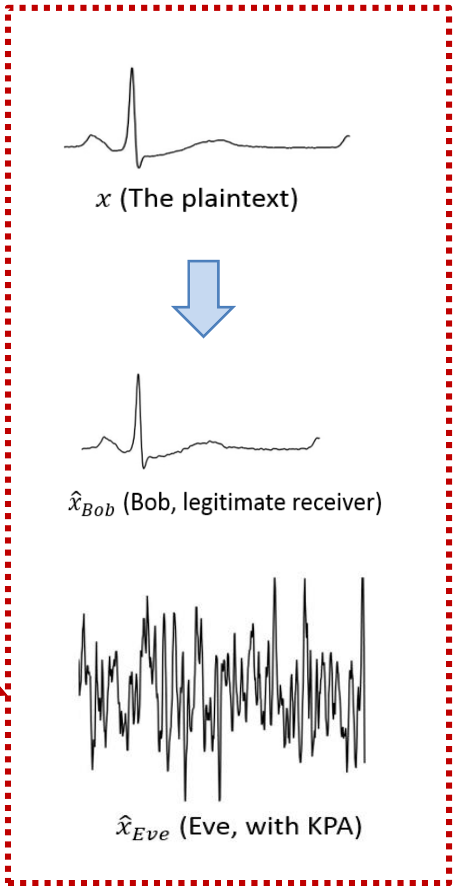


Simulation Result under Known-Plaintext Attack (KPA)









Proposed model:

Can't be cracked even 1 day passed

Comparison

	Prior CS-based Privacy Preserving [18-21]	**Proposed CS-based Privacy Preserving**
Mechanism	Multiple sensing matrices	Multiple watermarks
Ciphertext-Only Attack (COA)	norm (y) ∝ norm(x)	Disturb energy of ***y***
	Leak energy info.	Preserve energy info.
Known-Plaintext Attack (KPA)	Need Synchronization	Do not need Sync.
	Φ are leaked within 1Hr.	Sustain more than one day.
PRNG capability	Generate $512 \times 128 \times 8 = 524{,}288\ bits$ (e.g. 8 of Φ)	Generate $128 \times 6 \times 8 = 6{,}144\ bits$ (e.g. 8 of ***W***)

Comparison

	Prior CS-based Privacy Preserving [18-21]	Proposed CS-based Privacy Preserving
Mechanism	Multiple sensing matrices	Multiple watermarks
PRNG capability	Generate $512 \times 128 \times 8 = 524{,}288\ bits$ (e.g. 8 of Φ)	Generate $128 \times 6 \times 8 = 6{,}144\ bits$ (e.g. 8 of ***W***)
Ciphertext-Only Attack (COA)	norm (y) ∝ norm(x)	Disturb energy of ***y***
	Leak energy info.	Preserve energy info.
Known-Plaintext Attack (KPA)	Need Synchronization	Do not need Sync.
	are leaked within 1Hr.	Sustain more than one day.

Summary: Low-complexity Watermark Encryption for CS-based Privacy Preserving

- **Front-end Sensor:** **low-complexity** watermark encryption
  - CA provide pre-defined watermark w/ only m dimension
  - Randomly insert selected watermark
  - Save ***more than 99%*** of generated bit from PRNG
  - Watermarks hide energy information: ***cope with COA effectively***
- **Back-end Solver:** watermark removing **w/o synchronization**
  - CA provide pre-defined dictionary-based decrypting basis
  - Perform reconstruction & watermark remove simultaneously
  - Relieve synchronization issue: ***cope with KPA effectively***
- **Sample**, **compress** and **encrypt** simultaneously (**3-in-1!**)
  - Very suitable for emerging WSN in IoT w/ limited resource

Thank you!

Reference (1/3)

[1] Gubbi, Jayavardhana, et al. "Internet of Things (IoT): A vision, architectural elements, and future directions." *Future generation computer systems* 29.7 (2013): 1645-1660.

[2] Kelly, Sean Dieter Tebje, Nagender Kumar Suryadevara, and Subhas Chandra Mukhopadhyay. "Towards the implementation of IoT for environmental condition monitoring in homes." *IEEE Sensors Journal* 13.10 (2013): 3846-3853.

[3] Wang, Yuhao, et al. "Data-driven sampling matrix boolean optimization for energy-efficient biomedical signal acquisition by compressive sensing." *IEEE transactions on biomedical circuits and systems* 11.2 (2017): 255-266.

[4] Kung, Sun-Yuan. "Compressive Privacy: From Information\/Estimation Theory to Machine Learning [Lecture Notes]." IEEE Signal Processing Magazine 34.1 (2017): 94-112.

[5] F. Chen, A. P. Chandrakasan and V. M. Stojanovic, "Design and analysis of a hardware-efficient compressed sensing architecture for data compression in wireless sensors," *IEEE J. Solid-State Circuits*, vol. 47, no. 3, pp. 744-756, Mar. 2012.

[6] M. Unser, “Sampling-50 years after Shannon,” *Proc. IEEE*, vol. 88, no. 4, pp. 569–587, 2000.

[7] E. Gluskin, “Norms of random matrices and widths of finite-dimensional sets,” *Math. USSR-Sbornik*, vol. 48, pp. 173-183, 1984.

[8] D. L. Donoho, “Compressed sensing,” *IEEE Trans. Inf. Theory*, vol.52, no. 4, pp. 1289–1306, Apr. 2006.

[9] E. J. Candes and M. B. Wakin, “An Introduction to Compressive Sampling,” *IEEE Signal Processing Magazine*, vol. 25, no. 2, pp.21-30, Mar. 2008.

Reference (2/3)

[10] H. Mamaghanian, N. Khaled, D. Atienza and P. Vandergheynst, "Compressed Sensing for Real-Time Energy-Efficient ECG Compression on Wireless Body Sensor Nodes," in *IEEE Transactions on Biomedical Engineering*, vol. 58, no. 9, pp. 2456-2466, Sept. 2011.

[11] J. Zhang, D. Zhao, C. Zhao, R. Xiong, S. Ma and W. Gao, "Image Compressive Sensing Recovery via Collaborative Sparsity," in *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 2, no. 3, pp. 380-391, Sept. 2012.

[12] Agrawal, Shweta, and Sriram Vishwanath. "Secrecy using compressive sensing." *Information Theory Workshop (ITW)*, 2011 IEEE. IEEE, 2011.

[13] Rachlin, Yaron, and Dror Baron. "The secrecy of compressed sensing measurements." *Communication, Control, and Computing, 2008 46th Annual Allerton Conference on. IEEE*, 2008.

[14] Abdulghani, Amir M., and Esther Rodriguez-Villegas. "Compressive sensing: from “compressing while sampling” to “compressing and securing while sampling”." *Engineering in Medicine and Biology Society (EMBC*), 2010 Annual International Conference of the IEEE. IEEE, 2010.

[15] Orsdemir, Adem, et al. "On the security and robustness of encryption via compressed sensing." *Military Communications Conference*, 2008. *MILCOM* 2008. IEEE. IEEE, 2008.

[6] T. Bianchi, V. Bioglio and E. Magli, "Analysis of One-Time Random Projections for Privacy Preserving Compressed Sensing," in *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 2, pp. 313-327, Feb. 2016.

[17] Cambareri, Valerio, et al. "On known-plaintext attacks to a compressed sensing-based encryption: A quantitative analysis." *IEEE Transactions on Information Forensics and Security* 10.10 (2015): 2182-2195.

Reference (3/3)

[18] V. Cambareri, J. Haboba, F. Pareschi, H. R. Rovatti, G. Setti and K. w. Wong, "A two-class information concealing system based on compressed sensing," in *Proc. ISCAS*, 2013 May, pp. 1356-1359.

[19] V. Cambareri, M. Mangia, F. Pareschi, R. Rovatti, and G. Setti, “Low-complexity multiclass encryption by compressed sensing," *IEEE Trans. Sig. Proc. (TSP)*, vol. 63, no. 9, pp. 2183-2195, May 2015.

[20] Dautov, Ruslan, and Gill R. Tsouri. "Securing while sampling in wireless body area networks with application to electrocardiography." IEEE journal of biomedical and health informatics 20.1 (2016): 135-142.

[21] Fay, Robin, and Christoph Ruland. "Compressive Sensing encryption modes and their security." Internet Technology and Secured Transactions (ICITST), 2016 11th International Conference for. IEEE, 2016.

[22] R. Rubinstein, A. M. Bruckstein and M. Elad, "Dictionaries for Sparse Representation Modeling," in *Proceedings of the IEEE*, vol. 98, no. 6, pp. 1045-1057, June 2010.

[23] J. Mairal, F. Bach, J. Ponce, and G. Sapiro, "Online dictionary learning for sparse coding," in *Proc. International Conference on Machine Learning (ICML)*. Jun. 2009, pp. 689-696.