Energy Concealment based Compressive Sensing Encryption scheme for IoT

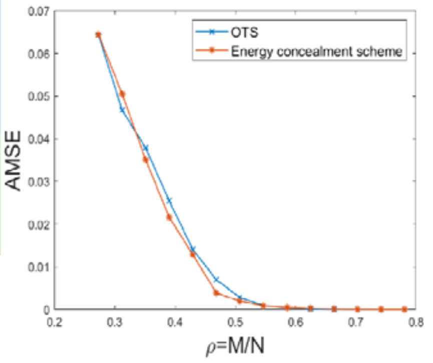
Gajraj Kuldeep, Qi Zhang Aarhus University, Denmark Email: {gkuldeep, qz}@eng.au.dk

We aim to design a lightweight energy efficient E2E information secrecy for IoT system, which can be implemented at resource-constrained IoT devices.

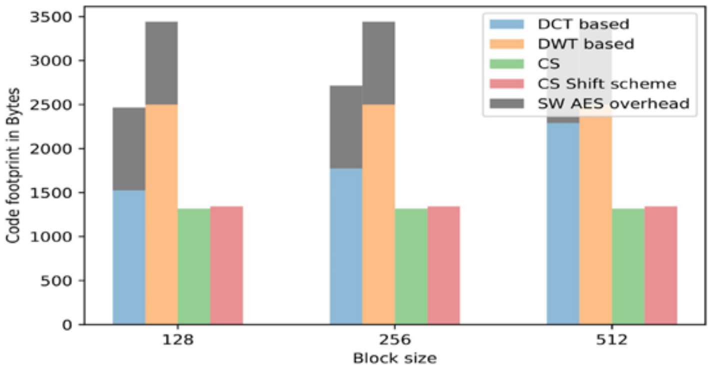
		Joint compression and encryption	Lightweight and energy efficiency	E2E info. secrecy for small data block size
AES		×	×	✓
SoA CS	Computationally secure	✓	Generation of Gaussian sensing matrix	Vulnerable for small length signal
	Perfect secrecy	✓	Generation of Gaussian sensing matrix	Detection of zero signal and need addition secure channel
EC scheme		✓	✓	✓

Proposed Energy concealment scheme

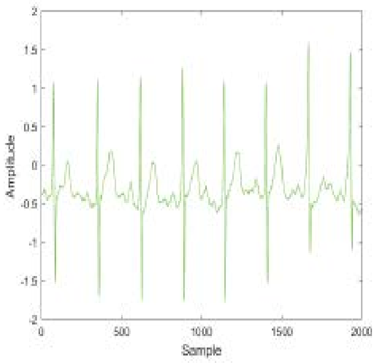
- ✓ Construction of constant energy signals to achieve asymptotic perfect secrecy
- ✓ Design of approximate Gaussian sensing matrices using energy efficient LFSR and NFSR
- ✓ Achieve end-to-end information secrecy for small block size signals
- ✓ Secure against ciphertext-only attack, known and chosen plaintext attacks
- ✓ Repeatability of the sensing matrix for small block size is 2^{200}
- ✓ Achieve better signal reconstruction performance compared to the SoA CS encryption schemes at the same compression ratio, or achieve better compression ratio at equivalent reconstruction performance.



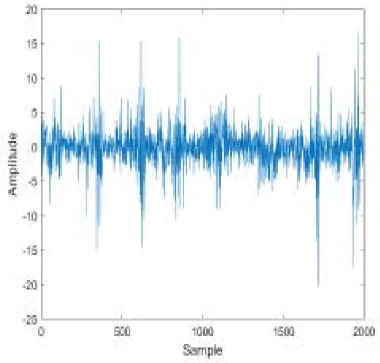
(a) Reconstruction performance



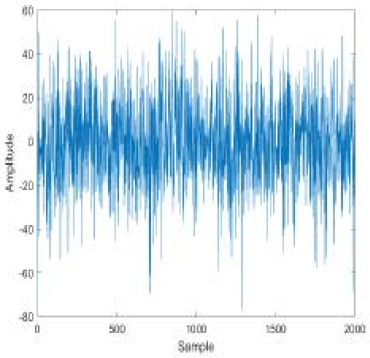
(b) Memory footprint



(a) ECG signal

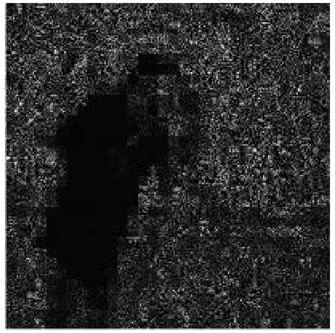


(b) Reconstructed signal from OTS scheme

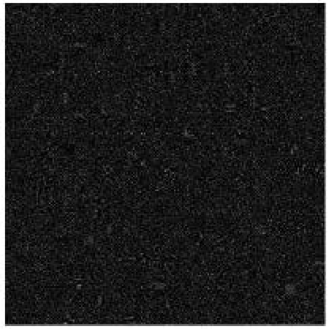


(c) Reconstructed signal from EC scheme

(a) Original image



(b) Reconstructed image from EOS scheme



(c) Reconstructed image from EC scheme

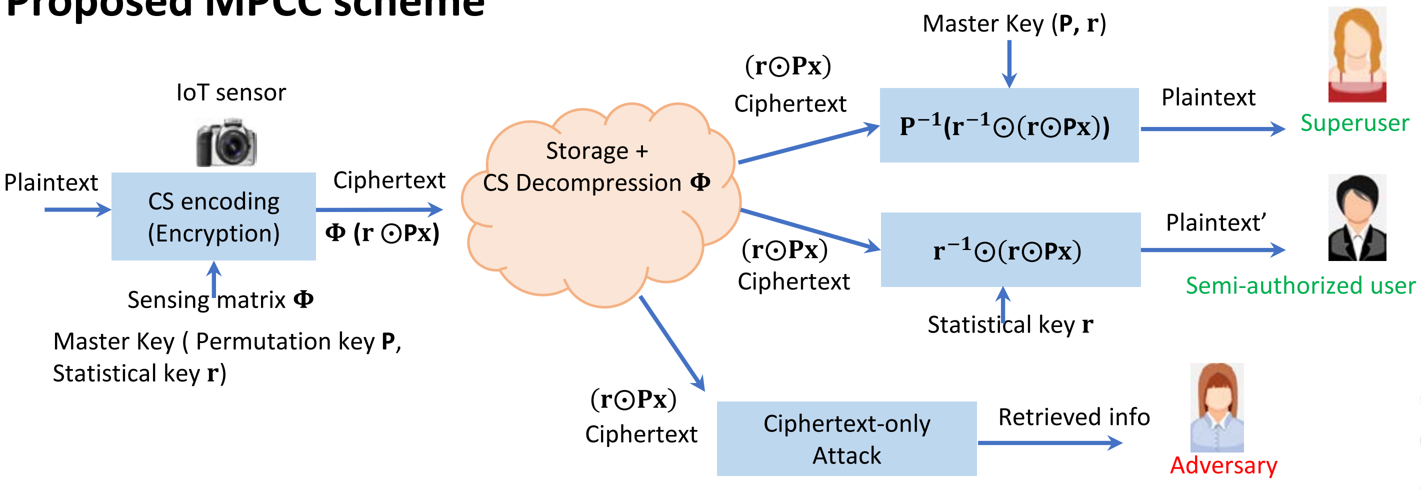
The designed EC scheme achieves information secrecy equivalent to symmetric key encryption with lightweight and energy efficient computations.

Compressive Sensing based Multi-class Privacy-preserving Cloud Computing (MPCC)

Gajraj Kuldeep, Qi Zhang Aarhus University, Denmark Email: {gkuldeep, qz}@eng.au.dk

We aim to design a joint compression and information secrecy scheme with multi-class encryption feature and allowing privacy preserving computationally intensive signal recovery at cloud.

Proposed MPCC scheme

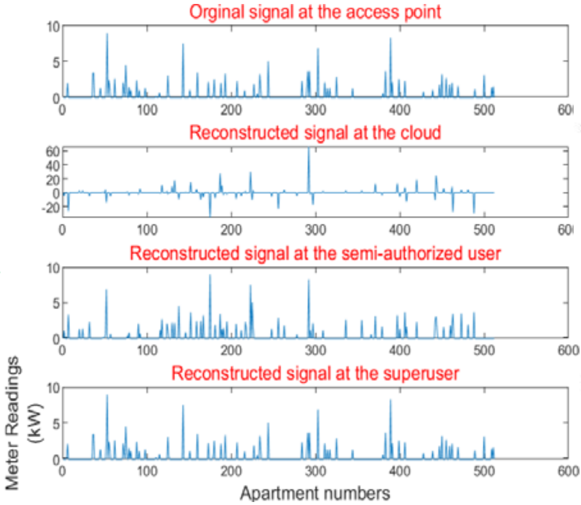

IoT sensor
Plaintext
CS encoding (Encryption)
Ciphertext
Φ (r ⊙Px)
Sensing matrix Φ
Master Key (Permutation key **P**, Statistical key **r**)
Storage + CS Decompression Φ
$(\mathbf{r}\odot\mathbf{Px})$
Ciphertext
Master Key (**P**, **r**)
$\mathbf{P}^{-1}(\mathbf{r}^{-1}\odot(\mathbf{r}\odot\mathbf{Px}))$
Plaintext
Superuser
$(\mathbf{r}\odot\mathbf{Px})$
Ciphertext
$\mathbf{r}^{-1}\odot(\mathbf{r}\odot\mathbf{Px})$
Plaintext'
Semi-authorized user
Statistical key **r**
$(\mathbf{r}\odot\mathbf{Px})$
Ciphertext
Ciphertext-only Attack
Retrieved info
Adversary

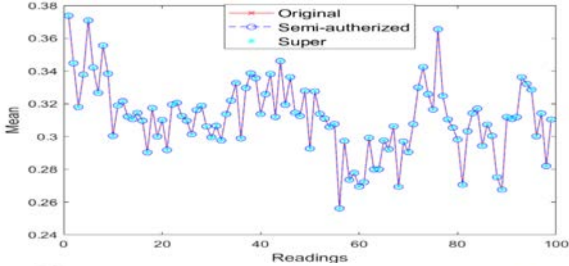
- ✓ Achieve joint compression and information secrecy for resource-constrained IoT devices
- ✓ Computational intensive signal recovery is performed at cloud while preserving data privacy and information secrecy.
- ✓ Multi-class encryption achieved using accessibility of key
  - ✓ Superuser can retrieve complete signal
  - ✓ Semi-authorized user can retrieve only statistical information
- ✓ Reconstruction performance is equivalent to the SoA CS encryption schemes

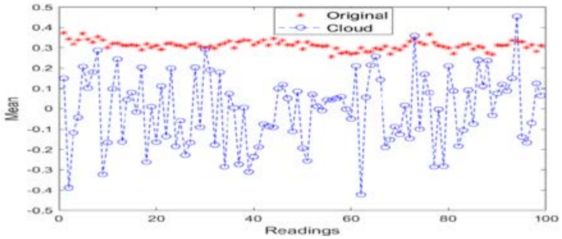
Performance comparison

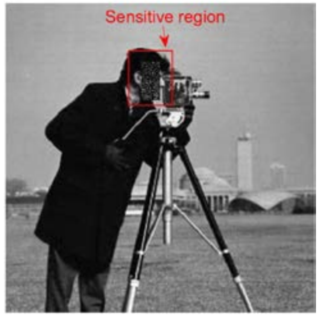
	LPCSDG	CSDGS	MC_ECG	MCI	MPCC
Cloud storage cost (in Bytes)	$O(2N)$	$O(N)$	$O(M)$	$O(M)$	$O(M)$
Sensor data Transmission	$O(M)$	$O(M)$	$O(M)$	$O(M)$	$O(M)$
Sensor computation	$O(MN)$	$O(MN)+[\Psi]$	$O(MN)$	$O(MN)$	$O(MN)+[\Psi]$
Data transmission for query from superuser	$O(MN)$	Simple query	N/A	N/A	Simple query
Superuser computation (in operation)	$O(N^{\theta})$ $2<\theta<3$	$O(N)+[\Psi]$	$O(N^3)$	$O(N^3)$	$O(N)+[\Psi]$
Privacy protection	Permuted index of data	Permuted and changed value	CS	CS+ Watermarking	Permuted and changed value
Semi-authorized user	N/A	N/A	$O(N^3)$	$O(N^3)$	$O(N)+[\Psi]$

Application of MPCC on smart meter data and images



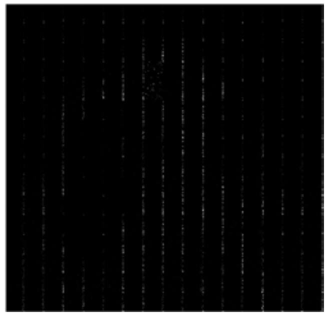






(a) Reconstructed image at semi-authorized user

(b) Reconstructed image at superuser



(c) Reconstructed image at cloud

The MPCC scheme achieves multi-class encryption with privacy preserving signal recovery at cloud for resource-constrained IoT devices.