On the Indistinguishability of Compressed Encryption With Partial Unitary Sensing Matrices

Nam Yul Yu

Gwangju Institute of Science and Technology (GIST), Korea

IEEE Global Conference on Signal and Information Processing (GlobalSIP)
Montreal, Canada

Nov. 15, 2017

This work was supported by the National Research Foundation of Korea (NRF).

CS-based Cryptosystems

- **Security for IoT and M2M**
  - Security issues are major challenges for the Internet-of-Things (IoT) and M2M communications.
  - Security techniques with **low latency**, **low power consumption**, and **low complexity** are required.

- **Compressed Sensing (CS) based Cryptosystems**
  - **Simultaneous sensing** and **encryption**
  - Efficient encryption/decryption
  - Reliability and security
  - Low complexity and low power consumption

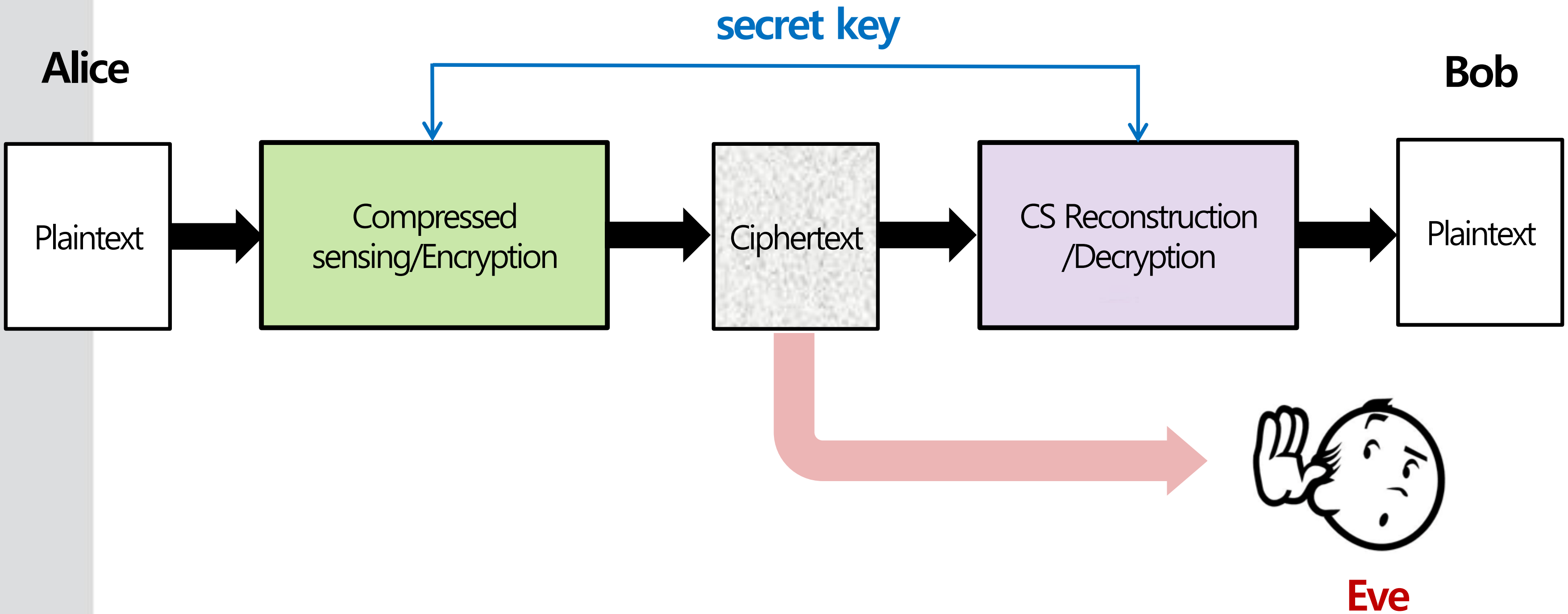
CS-based Cryptosystems

- History
  - **Hint [Candes&Tao'06]**
    : CS measurement samples are *weakly encrypted*.
  - **Kick-off [Rachlin&Baron'08]**
    : CS-based cryptosystems cannot be *perfectly secure*, but can be computationally secure.
  - **Kick-off [Orsdemir *et al.*'08]**
    : Demonstrated that CS-based cryptosystems can be computationally secure.
  - **Gaussian one-time sensing (G-OTS) cryptosystem [Bianchi *et al.*'14]**
    : perfectly secure, as long as each plaintext has constant energy
  - **Random Bernoulli based cryptosystem [Cambareri *et al.*'15]**
    : CS-based cryptosystem for multiclass encryption

  - Many other research works for practical applications
    : smart grids, image encryption, wireless communications, etc.

CS-based Cryptosystems

- Symmetric-key CS-based Cryptosystems

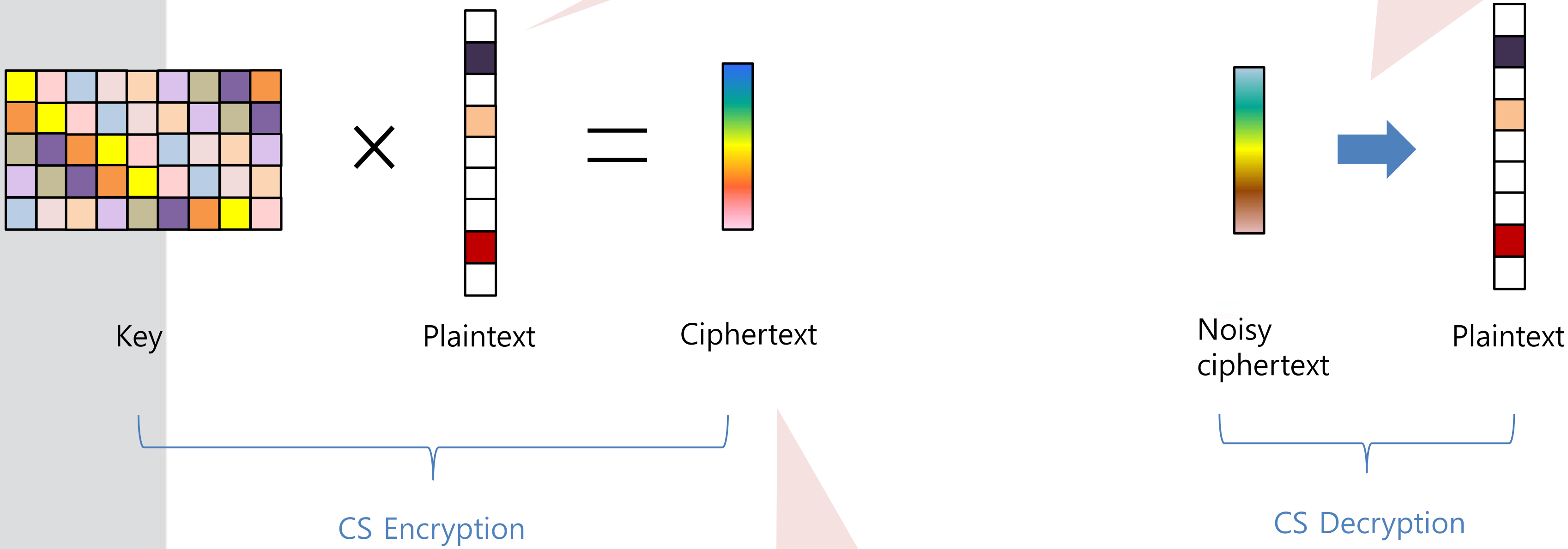


CS-based Cryptosystems

- **CS Encryption/Decryption**

Each plaintext is sparse with respect to an arbitrary basis.

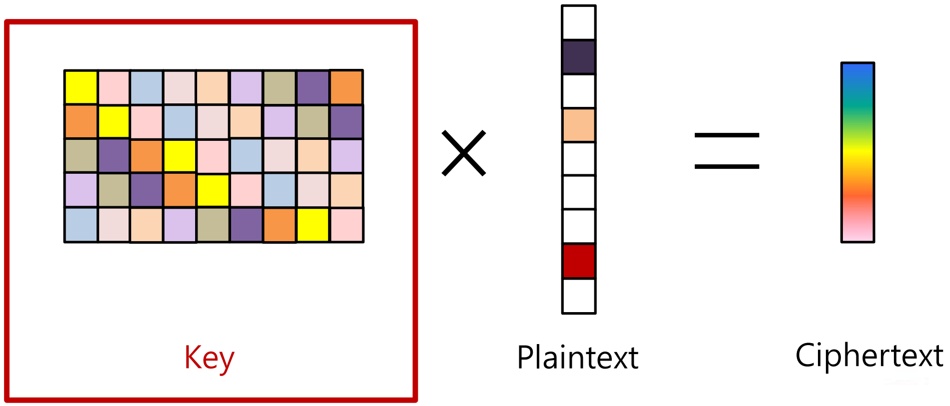
CS recovery algorithms are applied for CS decryption.



Key: M x N matrix
Plaintext: N x 1 vector
Ciphertext: M x 1 vector

CS-based Cryptosystems

- Gaussian One-Time Sensing (G-OTS) Cryptosystem



Φ: **random Gaussian matrix**

One-time sensing is crucial for CPA-security.

– **One-time sensing**: a random Gaussian matrix is used only once, and renewed for each encryption.

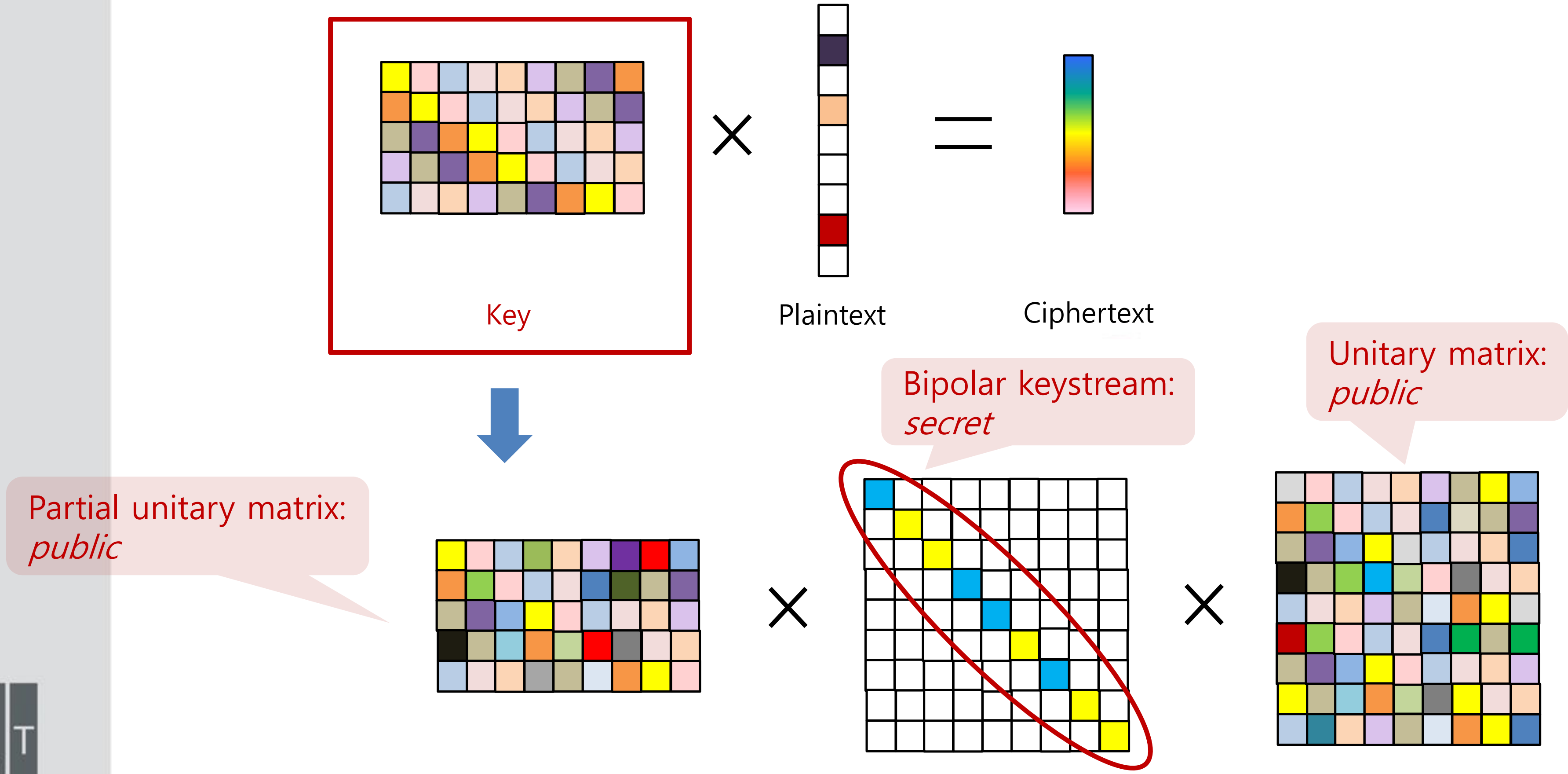
CS-based Cryptosystems

- **Gaussian One-Time Sensing (G-OTS) Cryptosystem**
  - **Pros**
    - The G-OTS cryptosystem reveals only the energy of the plaintext.
    - Thus, it is *perfectly secure,* as long as each plaintext has constant energy.
  - **Cons**
    - Each CS encryption/decryption requires *high complexity* and *processing time* by matrix-vector multiplication with Gaussian distributed elements.
    - M x N Gaussian distributed elements are required for each encryption.

The motivation of this work is to overcome the practical concerns.

Proposed CS-based Cryptosystems

- **Proposed CS encryption**



Proposed CS-based Cryptosystems

- Mathematical Formulation

$$\boxed{\mathbf{\Phi} = \frac{1}{\sqrt{M}}\mathbf{R}_\Omega\mathbf{U} = \frac{1}{\sqrt{MN}}\mathbf{R}_\Omega\mathbf{U}_1\mathrm{diag}(\mathbf{s})\mathbf{U}_2}$$

  - **$\mathbf{U}_1$ = H:** Each entry of $\mathbf{U}_1$ should have unit magnitude.

$$\mathbf{H}(k,t) = \begin{cases} 1, & \text{if } k=0 \text{ or } t=0, \\ (-1)^{d_{k+t-2}}, & \text{otherwise} \end{cases}$$

d is a binary *m*-sequence.

  - **$\mathbf{U}_2$: Unitary matrix**
  - **s: secret bipolar keystream**
    - LFSR-based keystream
    - *Example*: Self-shrinking generator (SSG)

The secret keystream bits can be generated fast and efficiently.

Proposed CS-based Cryptosystems

- **Practical Benefits**
  - **Efficient keystream usage**
    - G-OTS cryptosystem: M x N real-valued elements required for each encryption
    - Proposed cryptosystem: N keystream bits required for each encryption
  - **Fast and efficient keystream generation**: The original keystream can be efficiently generated by an LFSR-based keystream generator.
  - **Fast and efficient CS encryption/decryption**: By employing unitary matrices, matrix-vector multiplications for CS processes can be efficiently implemented.
- **Reliability**
  - **Stable** and **robust CS decryption:** A plaintext with at most K nonzero entries can be decrypted with bounded errors by a legitimate recipient, as long as

$$M = \mathcal{O}(K\log^5 N)$$

Security Analysis

- **Indistinguishability**
  - If a cryptosystem has the indistinguishability, no eavesdropper can learn any partial information about the plaintext from a given ciphertext.
  - The indistinguishability formalizes the notion of **computational security** of a cryptosystem.
  - The indistinguishability is measured by the success probability of an adversary in the **indistinguishability experiment**.

Security Analysis

- **Indistinguishability Experiment (for a CS-based cryptosystem)**

Step 1:	An adversary creates a pair of plaintexts $\mathbf{x}_1$ and $\mathbf{x}_2$ of the same length, and submits them to a CS-based cryptosystem.
Step 2:	The CS-based cryptosystem encrypts a plaintext $\mathbf{x}_h$ by randomly selecting $h \in \{1, 2\}$, and gives a noisy ciphertext $\mathbf{r} = \mathbf{\Phi}\mathbf{x}_h + \mathbf{n}$ back to the adversary.
Step 3:	Given the ciphertext $\mathbf{r}$, the adversary carries out a polynomial time test $\mathcal{D} : \mathbf{r} \rightarrow h' \in \{1, 2\}$, to figure out the corresponding plaintext.
Decision:	The adversary passes the experiment if $h' = h$, or fails otherwise.

- If no adversary passes the indistinguishability experiment in polynomial time with probability significantly better than that of a random guess, the cryptosystem is said to have the indistinguishability.

Security Analysis

- **Total Variation (TV) Distance**

$$d_{\mathrm{TV}}(\mu,\nu) = \sup_{A\subset\Omega}|\mu(A)-\nu(A)|$$

  - μ,ν: probability measures on Ω

– The success probability of an adversary in the indistinguishability experiment

$$p_d \leq \frac{1}{2} + \frac{d_{\mathrm{TV}}(p_1,p_2)}{2}$$

  - $p_1 = \Pr(\mathbf{r}|\mathbf{x}_1)$ and $p_2 = \Pr(\mathbf{r}|\mathbf{x}_2)$

– The TV distance can be a statistical measure for indistinguishability.

Security Analysis

- **Hellinger Distance**

$$d_{\mathrm{H}}(\mu,\nu)=\left[\frac{1}{2}\int_{\Omega}\left(\sqrt{f(x)}-\sqrt{g(x)}\right)^2 dx\right]^{\frac{1}{2}}$$

  - f, g: densities of probability measures μ, ν on Ω

  – For multivariate normal with zero mean,

$$d_{\mathrm{H}}{}^2(p_1,p_2)=1-\frac{\det(\mathbf{C}_1)^{\frac{1}{4}}\det(\mathbf{C}_2)^{\frac{1}{4}}}{\det\left(\frac{\mathbf{C}_1+\mathbf{C}_2}{2}\right)^{\frac{1}{2}}}$$

  - $\mathbf{C}_1$ and $\mathbf{C}_2$: Covariance matrices of $\mathbf{r}$ conditioned on $\mathbf{x}_1$ and $\mathbf{x}_2$

Security Analysis

- **TV and Hellinger distances**

$$d_{\mathrm{H}}{}^{2}(p_1,p_2) \le d_{\mathrm{TV}}(p_1,p_2) \le d_{\mathrm{H}}(p_1,p_2)\sqrt{2-d_{\mathrm{H}}{}^{2}(p_1,p_2)}$$

Theorem: In the proposed CS-based cryptosystem, if each plaintext $\mathbf{x}$ has at most K nonzero elements with constant energy $\mathcal{E}_x$, then

$$d_{\mathrm{H}}(p_1,p_2) \le \sqrt{1-\left(\frac{2\sqrt{K\mu^2(\mathbf{U}_2)\cdot \mathrm{PNR}+1}}{K\mu^2(\mathbf{U}_2)\cdot \mathrm{PNR}+2}\right)^{\frac{M}{4}}}$$

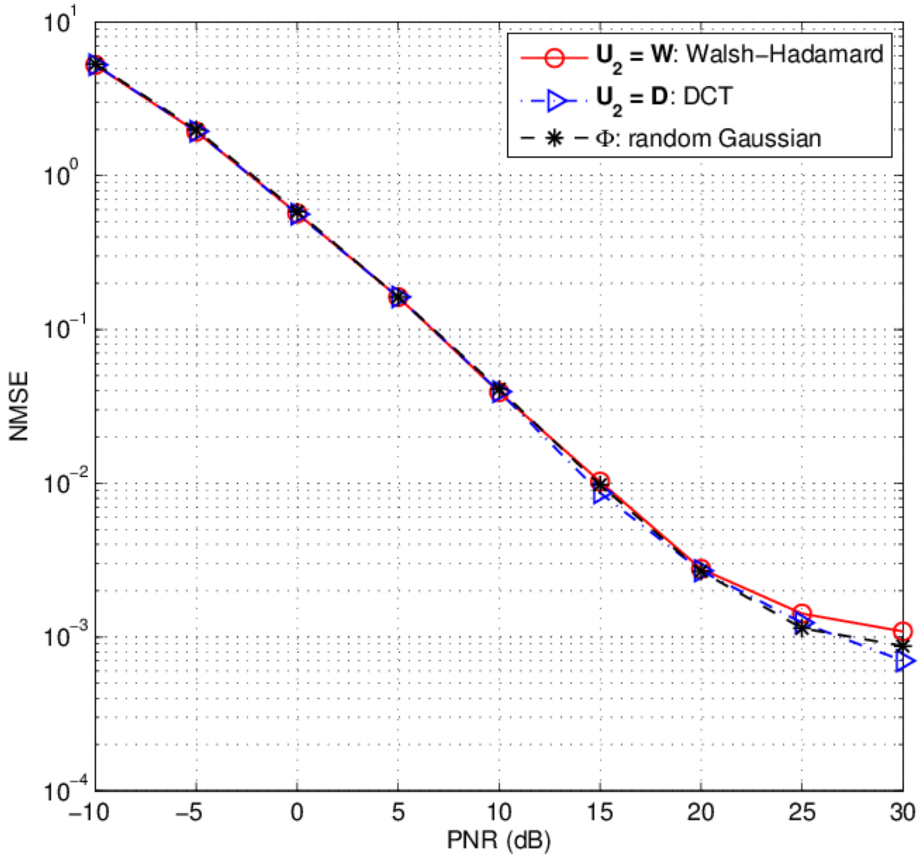
where $\mathrm{PNR}=\frac{\mathcal{E}_x}{M\sigma^2}$ and $\mu(\mathbf{U}_2)$ is the maximum magnitude of the entries of $\mathbf{U}_2$.

GIST

Numerical Results

- **Reliability**

For a legitimate recipient, the proposed CS-based cryptosystem is as reliable as the random Gaussian sensing.

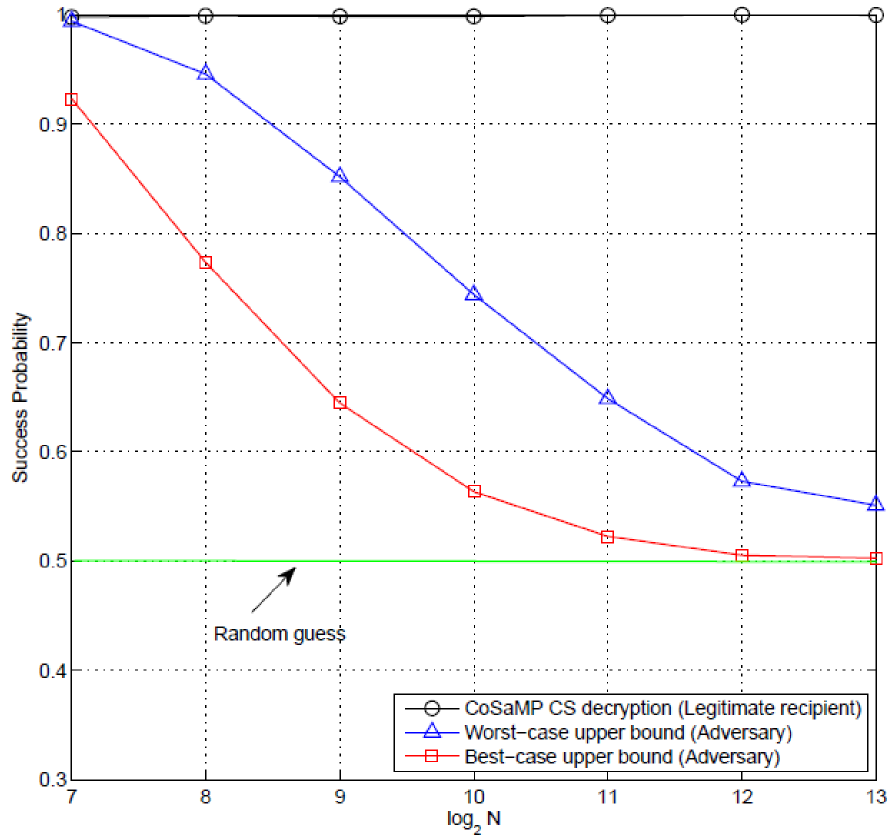


- N = 1024
- M = 48
- K = 4

Numerical Results

- **Success probabilities**

For a given M, the adversary's success probability approaches that of a random guess as N increases.

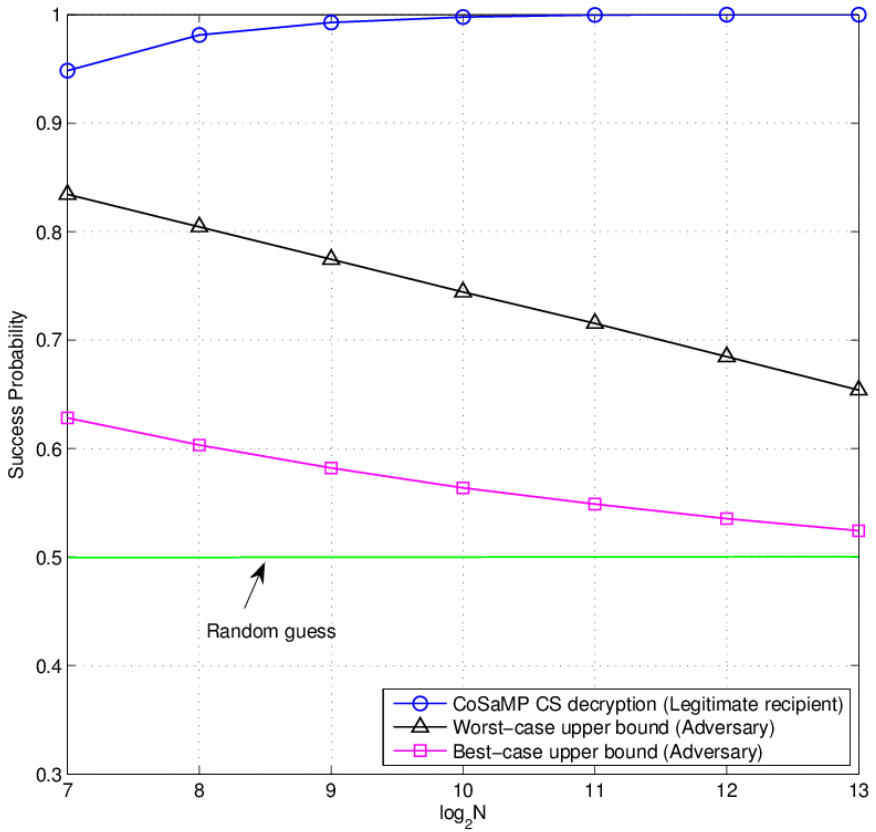


- PNR = 25 dB
- M = 48
- $K = \left\lfloor \frac{8.5M}{\log_2^2 N} \right\rfloor$

Numerical Results

- **Success probabilities**

For a given K, the adversary's success probability approaches that of a random guess as N increases.



- PNR = 25 dB
- K = 4
- $M = \lceil 0.12 K \log_2^2 N \rceil$

Conclusions

- **Proposed CS-based cryptosystem**
  - CS-based cryptosystem with partial unitary matrices embedding a secret bipolar keystream
  - Theoretically guarantees **reliable decryption** for a legitimate recipient.
  - Demonstrates the potential of **computational security** against an eavesdropper, if the keystream is sufficiently long with low compression and sparsity ratios.
  - Practical benefits
    - **Efficient usage of cryptographic primitives** by embedding a short keystream.
    - **Fast and efficient keystream generation** by LFSR-based keystream generators.
    - **Fast and efficient CS encryption/decryption** by employing unitary matrices.

Thank You!