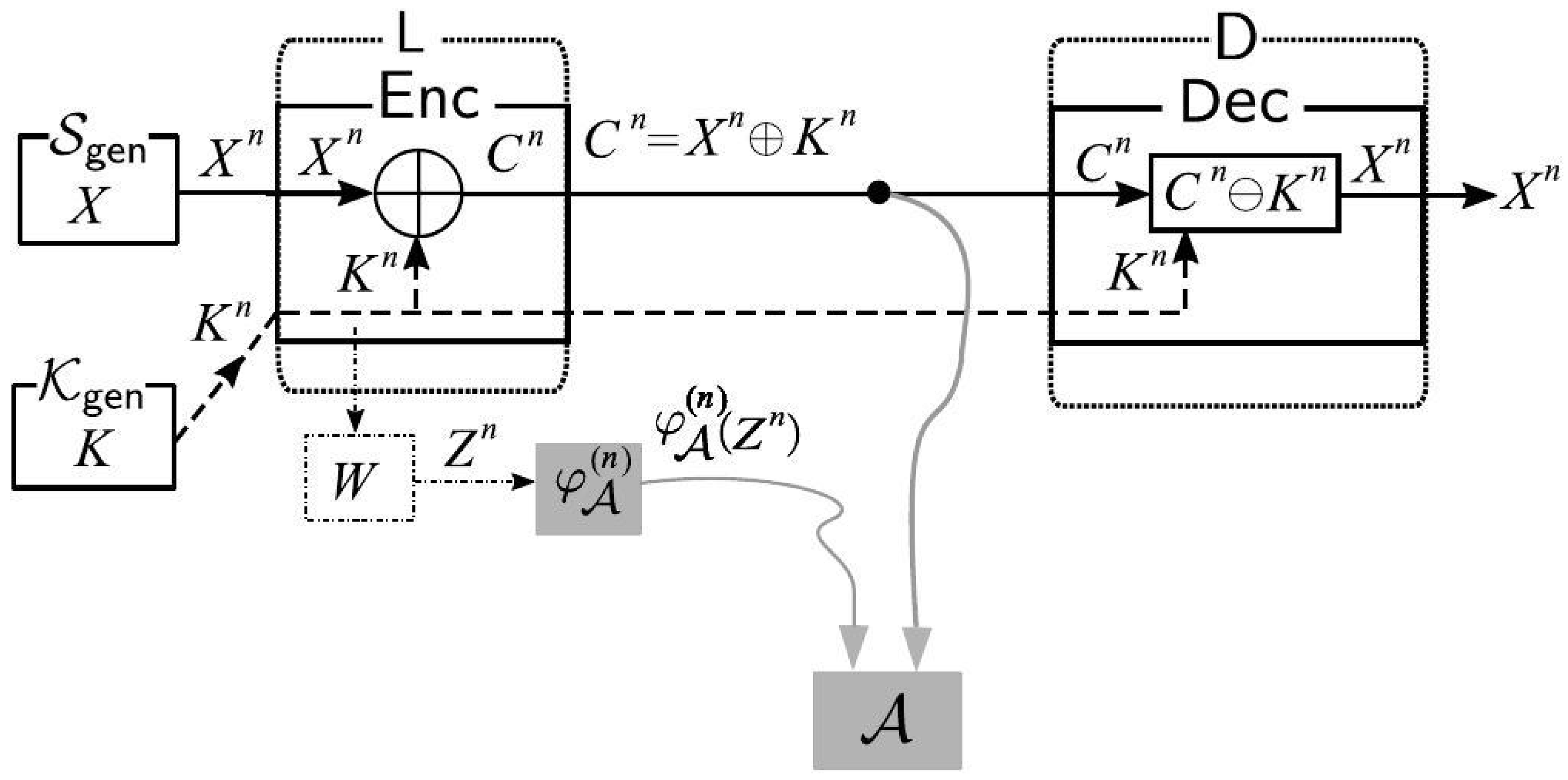

Fig. 1. Side-channel attacks to the Shannon cipher system.

1) *Source Processing:* At the node , X^n is encrypted with the key K^n using the encryption function Enc. The ciphertext C^n of X^n is given by $C^n := \mathsf{Enc}(X^n) = X^n \oplus K^n$.
2) *Transmission:* Next, the ciphertext C^n is sent to the information processing center D through a *public* communication channel. Meanwhile, the key K^n is sent to D through a *private* communication channel.
3) *Sink Node Processing:* In D, we decrypt the ciphertext C^n using the key K^n through the corresponding decryption procedure Dec defined by $\mathsf{Dec}(C^n) = C^n \ominus K^n$. It is obvious that we can correctly reproduce the source output X^n from C^n and K^n by the decryption function Dec.

Side-Channel Attacks by Eavesdropper Adversary:

An *(eavesdropper) adversary* $\mathcal{A}$ eavesdrops the public communication channel in the system. The adversary $\mathcal{A}$ also uses a side information obtained by side-channel attacks. Let $\mathcal{Z}$ be a finite set and let $W : \mathcal{X} \to \mathcal{Z}$ be a noisy channel. Let Z be a channel output from W for the input random variable K. We consider the discrete memoryless channel specified with W. Let $Z^n \in \mathcal{Z}^n$ be a random variable obtained as the channel output by connecting $K^n \in \mathcal{X}^n$ to the input of channel. We write a conditional distribution on Z^n given K^n as

$$W^n = \{W^n(z^n|k^n)\}_{(k^n,z^n)\in\mathcal{K}^n\times\mathcal{Z}^n} .$$

Since the channel is memoryless, we have

$$W^n(z^n|k^n) = \prod_{t=1}^{n} W(z_t|k_t). \tag{1}$$

On the above output Z^n of W^n for the input K^n, we assume the followings.

- The three random variables X, K and Z, satisfy $X \perp (K,Z)$, which implies that $X^n \perp (K^n, Z^n)$.
- W is given in the system and the adversary $\mathcal{A}$ can not control W.
- By side-channel attacks, the adversary $\mathcal{A}$ can access Z^n.

We next formulate side information the adversary $\mathcal{A}$ obtains by side-channel attacks. For each $n = 1, 2, \cdots$, let $\varphi_{\mathcal{A}}^{(n)} : \mathcal{Z}^n \to \mathcal{M}_{\mathcal{A}}^{(n)}$ be an encoder function. Set $\varphi_{\mathcal{A}} := \{\varphi_{\mathcal{A}}^{(n)}\}_{n=1,2,\cdots}$. Let

$$R_{\mathcal{A}}^{(n)} := \frac{1}{n}\log||\varphi_{\mathcal{A}}|| = \frac{1}{n}\log|\mathcal{M}_{\mathcal{A}}^{(n)}|$$

be a rate of the encoder function $\varphi_{\mathcal{A}}^{(n)}$. For $R_{\mathcal{A}} > 0$, we set

$$\mathcal{F}_{\mathcal{A}}^{(n)}(R_{\mathcal{A}}) := \{\varphi_{\mathcal{A}}^{(n)} : R_{\mathcal{A}}^{(n)} \le R_{\mathcal{A}}\}.$$

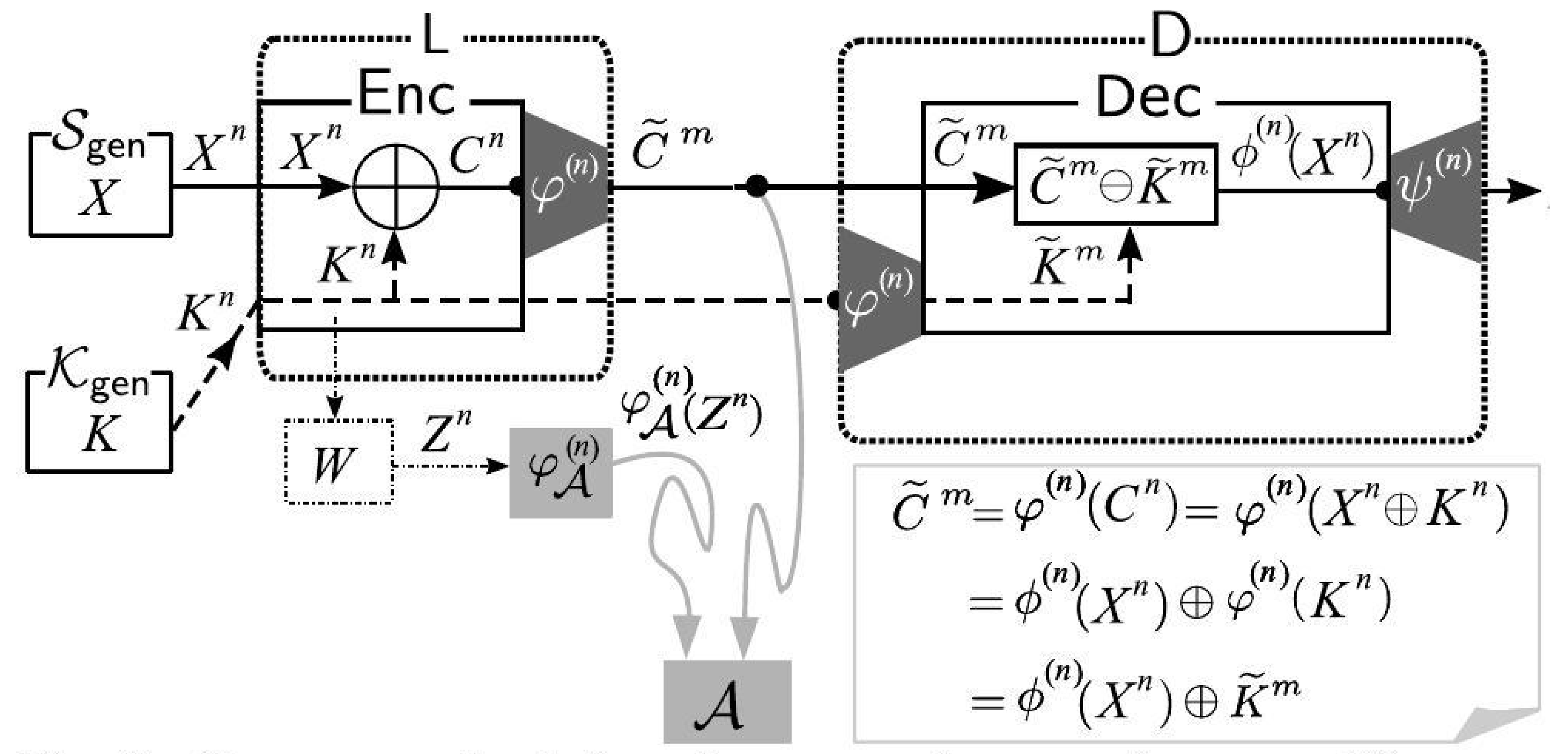

Fig. 2. Our proposed solution: linear encoders as privacy amplifiers.

On encoded side information the adversary $\mathcal{A}$ obtains we assume the following.

- The adversary $\mathcal{A}$, having accessed Z^n, obtains the encoded additional information $\varphi_{\mathcal{A}}^{(n)}(Z^n)$. For each $n = 1, 2, \cdots$, the adversary $\mathcal{A}$ can design $\varphi_{\mathcal{A}}^{(n)}$.
- The sequence $\{R_{\mathcal{A}}^{(n)}\}_{n=1}^{\infty}$ must be upper bounded by a prescribed value. In other words, the adversary $\mathcal{A}$ must use $\varphi_{\mathcal{A}}^{(n)}$ such that for some $R_{\mathcal{A}}$ and for any sufficiently large n, $\varphi_{\mathcal{A}}^{(n)} \in \mathcal{F}_{\mathcal{A}}^{(n)}(R_{\mathcal{A}})$.

C. Proposed Idea: Affine Encoder as Privacy Amplifier

For each $n = 1, 2, \cdots$, let $\phi^{(n)} : \mathcal{X}^n \to \mathcal{X}^m$ be a linear mapping. We define the mapping $\phi^{(n)}$ by

$$\phi^{(n)}(x^n) = x^n A \text{ for } x^n \in \mathcal{X}^n, \tag{2}$$

where A is a matrix with n rows and m columns. Entries of A are from $\mathcal{X}$. We fix $b^m \in \mathcal{X}^m$. Define the mapping $\varphi^{(n)} : \mathcal{X}^n \to \mathcal{X}^m$ by

$$\begin{aligned}\varphi^{(n)}(k^n) :=& \phi^{(n)}(k^n) \oplus b^m \\ =& k^n A \oplus b^m, \text{ for } k^n \in \mathcal{X}^n.\end{aligned} \tag{3}$$

The mapping $\varphi^{(n)}$ is called the affine mapping induced by the linear mapping $\phi^{(n)}$ and constant vector $b^m \in \mathcal{X}^m$. By the definition (3) of $\varphi^{(n)}$, those satisfy the following affine structure:

$$\begin{aligned}&\varphi^{(n)}(y^n \oplus k^n)(x^n \oplus k^n)A \oplus b^m = x^n A \oplus (k^n A \oplus b^m) \\ &= \phi^{(n)}(x^n) \oplus \varphi^{(n)}(k^n), \text{ for } x^n, k^n \in \mathcal{X}^n.\end{aligned} \tag{4}$$

Next, let $\psi^{(n)}$ be the corresponding decoder for $\phi^{(n)}$ such that $\psi^{(n)} : \mathcal{X}^m \to \mathcal{X}^n$. Note that $\psi^{(n)}$ does not have a linear structure in general.

Description of Proposed Procedure:

We describe the procedure of our privacy amplified system as follows.

1) *Encoding of Ciphertext:* First, we use $\varphi^{(n)}$ to encode the ciphertext $C^n = X^n \oplus K^n$. Let $\widetilde{C}^m = \varphi^{(n)}(C^n)$. Then, instead of sending C^n, we send $\widetilde{C}^m$ to the public communication channel. By the affine structure (4) of encoder we have that

$$\begin{aligned}\widetilde{C}^m &= \varphi^{(n)}(X^n \oplus K^n) \\ &= \phi^{(n)}(X^n) \oplus \varphi^{(n)}(K^n) = \widetilde{X}^m \oplus \widetilde{K}^m,\end{aligned} \tag{5}$$

where we set $\widetilde{X}^m := \phi^{(n)}(X^n), \widetilde{K}^m := \varphi^{(n)}(K^n)$.