A Physical Layer Endogenous Security Architecture with Dynamic Slicing Encryption for IoT

Journal:	*IEEE Internet of Things Journal*
Manuscript ID	IoT-41406-2024.R1
Manuscript Type:	Regular Article (S1)
Date Submitted by the Author:	25-Jan-2025
Complete List of Authors:	Ye, Xiaokai; Southeast University - Sipailou Campus, Electronics Engineering Lv, Tao; Southeast University - Sipailou Campus, Electronics Engineering Huang, Kun; Southeast University - Sipailou Campus, Electronics Engineering Li, Jinhui; Nanjing Xiguang Research Institute for Information Technology Shan, Xuekang; Nanjing Xiguang Research Institute for Information Technology Xiang, Wei; La Trobe University, School of Engineering and Mathematical Sciences Sun, Xiaohan; Southeast University - Sipailou Campus, Electronics Engineering
Keywords:	Network Architecture < Sub-Area 2: Communications and Networking for IoT, Secure Communications < Sub-Area 2: Communications and Networking for IoT, physical layer endogenous security

A Physical Layer Endogenous Security Architecture with Dynamic Slicing Encryption for IoT

Xiaokai Ye, Tao Lv, Kun Huang, Jinhui Li, Xuekang Shan, Wei Xiang*, and Xiaohan Sun*

***Abstract*—We propose a novel physical layer endogenous security (PHY-ES) architecture with a dynamic slicing encryption (DSE) scheme for the physical layer of Internet of Things (IoT) systems. The proposed architecture not only supports the functions of the traditional Ethernet physical layer, but also provides both endogenous encryption and decryption functions for sensing data, based on sensing endogenous keys (SEKs). A SEK-based DSE scheme is also proposed, where the SEKs are generated by quantifying the randomness of the sensing data, without needing any external key sources, which can directly encrypt the sensing data in the physical layer. Based on the above, we present the algorithm for the scheme, and give its performance evaluation method with parameters of data life cycle (DLC), average cost (AC) and deciphering probability. The simulation results for the changes in the DLC and AC are obtained under different sensing data lengths. Finally, we build an experimental platform to validate the scheme by setting up an experimental system with two nodes at the lab. The testing results show that the scheme adapts to the PHY-ES architecture with high security and low overhead performance, and the suitable slicing length is approximately L=8×10^3 bits, which are almost consistent with the simulations. Compared with other schemes, the SEK-based DSE scheme can reduce the DLC and AC by about 42% and 35% on average, respectively. The architecture and the scheme proposed in this paper provide a unique and advantageous approach for secure access to massive heterogeneous sensing data in the physical layer of IoT.**

***Index Terms*—Internet of Things (IoT), physical layer endogenous security (PHY-ES), sensing endogenous keys (SEKs), dynamic slicing encryption (DSE).**

I. Introduction

INTERNET of Things (IoT), as one solution capable with the advantages of carrying a large number of users, is widely used in medical, industry, urban construction, and other fields [1, 2]. With the development of new IoT applications, such as mini-grid, smarter healthcare, autonomous vehicles, smart ocean, etc., an increasing number of sensors and actuators with different types and levels installed in the physical layer of IoT [3–5]. Although IoT has been using the traditional Ethernet architecture and forming similar network protocols and standards [6, 7], the difference is that the sensing data traffic in the uplink channels of IoT is far greater than the one in current communication access networks [8]. This is because a large number of physical devices and modules are placed in the physical layer, the requirements of timely aggregation, processing, conversion, and transmission of sensing data are needed. The authors of [9] and [10] respectively proposed protocols enabling sensors and actuators by controller and physical layer convergence with a special data frame format, to connect sensing data to the access nodes in an orderly and reliable manner. However, the above schemes or protocols based on the traditional architecture lack an independent security function layout and corresponding transmission control channels, and the current physical layer of IoT cannot secure the sensing data traffic of the uplink channels. Therefore, it is necessary to re-plan and re-construct the physical layer architecture of the IoT.

Meanwhile, how to protect the security of massive uplink sensing data produced at the physical layer of IoT is also important. Currently, many schemes for key generation and encryption in the physical layer have been proposed. Some schemes have been proposed to generate keys from external noise sources, which encrypt a data signal into a data noise signal and transmit it with a time difference with a pure noise signal in the channels [11, 12]. Meanwhile, some schemes using different chaotic systems to generate keys have also been presented, which encrypt the original data signals into noise-like signals for transmission [13, 14]. Moreover, a scheme has been proposed to mark the signal level by utilizing the quantum-noise of the quantum system as keys, which encrypts the data signal by hiding it in the noise [15]. Other than the above physical layer key generation and encryption schemes to ensure data security by improving the anti-interception of data signals in the transmission medium, the artificial intelligence and machine learning provide novel methods for securing the sensing data traffic [16, 17]. However, these proposals not only increase the instability of the physical layer of IoT, due to that fact that external key source systems are vulnerable to external interference, such as temperature and vibration, but also increase the complexity and overhead of the physical layer of IoT, attributed to the fact that all keys need to be synchronized between the source nodes and destination nodes.

To the best of the authors' knowledge, there exist no reports of a solution that combines suitable physical layer architectures and security functions without using external key source systems for IoT sensing data in the physical layer. Therefore, we propose a novel physical layer endogenous security (PHY-ES) architecture with sensing endogenous keys (SEKs) based dynamic slicing encryption (DSE) scheme for

This work was supported by the Fundamental Research Funds for the Central Universities of China under Grant no. 2242023k30014 and no. 2242024k30048, and the National Natural Science Foundation of China under Grant no. 61271206. (Corresponding authors: Xiaohan Sun; Wei Xiang)

Xiaokai Ye, Tao Lv, Kun Huang, and Xiaohan Sun are with the National Research Center for Optical Sensing/communications Integrated Networking, Southeast University, Nanjing 210096, China.

Wei Xiang is with the School of Computing, Engineering and Mathematical Sciences, La Trobe University, Melbourne, VIC 3086, Australia.

Jinhui Li and Xuekang Shan are with the Nanjing Xiguang Research Institute for Information Technology, Nanjing 210012, China.

IoT, not only supports basic physical layer functions, but also provides both endogenous encryption and decryption functions for sensing data. The security functions can be realized in the scheme with high security and low overhead, and verified by both simulations and experiments.

In a nutshell, the main contributions can be summarized as follows.

1) *PHY-ES Architecture Providing both Endogenous Encryption and Decryption Functions*: Re-plan and re-construct the physical layer architecture of IoT based on the compatibility with traditional Ethernet physical layer architecture. We design an endogenous security sublayer (ESS) to realize both endogenous encryption and decryption, divide three data links for encrypted sensing data, decrypted receiving data, and send data, as well as an independent transmission channel for control signal at PHY-ES.
2) *SEK-based DSE Scheme*: A SEK-based DSE scheme is proposed, where the SEKs are generated by quantifying the randomness of the sensing data, without the need for any external key sources to encrypt the sensing data in the physical layer directly. The encryption process of the scheme is divided into initial SEK generation, SEK matrix creation, disarrangement of both SEKs and sensing data, etc.
3) *Novel SEK-based DSE Algorithm and its Experimental Platform*: We establish a novel SEK-based DSE algorithm and verify its feasibility by simulations. Meanwhile, we build an experimental platform to validate the proposed scheme and algorithm. The experimental results are consistent with their simulation counterparts. Compared with other schemes, the SEK-based DSE scheme is able to reduce the data life cycle (DLC) and average cost (AC) by around 42% and 35% on average, respectively.

The remainder of this paper is organized as follows. Section II proposes the PHY-ES architecture and the SEK-based DSE scheme. Section III details the process, algorithm, and simulation for the scheme. Section IV presents the experimental approach and system and discusses the testing results. Finally, Section V concludes this article.

II. Architecture and Scheme

In this section we provide a solution that combines suitable physical layer architectures and security functions without using external key source for IoT sensing data in the physical layer of IoT. The PHY-ES architecture suitable for the generic scenario of IoT and the SEK-based DSE scheme are proposed.

A. PHY-ES Architecture for IoT

The PHY-ES architecture with both endogenous encryption and decryption functions for IoT systems is shown in Fig.1. In addition to supporting the basic functions of the traditional Ethernet physical layer architecture, such as transmission medium connection, encoding/decoding, serial-to-parallel conversion, etc. [18, 19], the novel architecture proposed here also provides both the endogenous encryption and decryption functions for sensing data. Thus, the architecture consists of sensing sublayer (SS), physical function sublayer (PFS), and

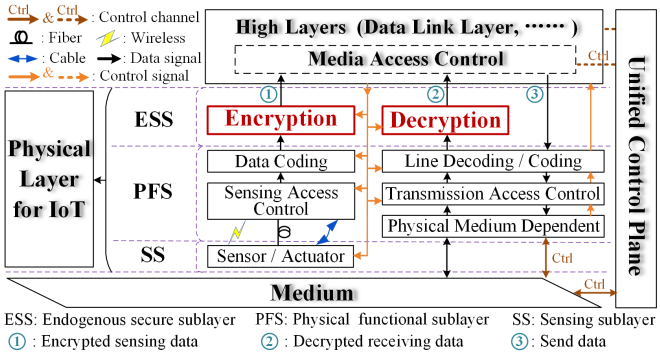


Fig. 1: PHY-ES architecture with both the endogenous encryption and decryption functions for IoT.

endogenous security sublayer (ESS). The control signals from the unified control plane are transmitted by an independent control channel, received by physical medium dependent, sent to higher layers, and then distributed to the corresponding functional modules at different functional sublayers. Thus, the control signals can directly manage the three sublayers at physical layer. For distinguishing between the control channels and control signals, the brown solid lines and dashed lines of Ctrl represent the actual and virtual control links, respectively, and the orange solid lines on the right and at the middle are the control signals, as shown in Fig.1.

The SS is composed of sensors and actuators for collecting sensing data and can be connected simultaneously with the PFS via optical fiber, cable, and wireless connections, or any one of them. The PFS provides connections between the SS and ESS, and between the medium and ESS, as well as provides access control, encoding/decoding, and other functions for sensing data. The ESS contains both endogenous encryption and decryption functions for generating SEKs without any external key source systems, encrypting and decrypting the sensing data directly at the physical layer.

There are many advantages of the PHY-ES architecture for the IoT. First, this architecture is highly compatible, providing both endogenous security functions and traditional physical layer functions. Then, the SEKs are generated directly from the sensing data accessed in the physical layer without any external key sources, so that the SEKs are not vulnerable to be interfered or intercepted by attackers, conducing to improve the security and stability and reduce the overhead for the physical layer. And both the encryption and decryption functions are transparent to the multi-source heterogeneous sensing data, and process the data with any length at one time, to enhance the flexibility of the physical layer. Finally, the SEK-based DSE scheme can encrypt huge amounts of multisource heterogeneous sensing data within the edge access nodes, adapt to the IoT networks with different size and changing environment, and has strong scalability.

B. SEK-based DSE Scheme

For achieving both the endogenous encryption and decryption functions of the PHY-ES architecture shown in Fig.1, a SEK-based DSE scheme implemented at the ESS is proposed in Fig.2. For ease of exposition, nodes n and m in Fig.2

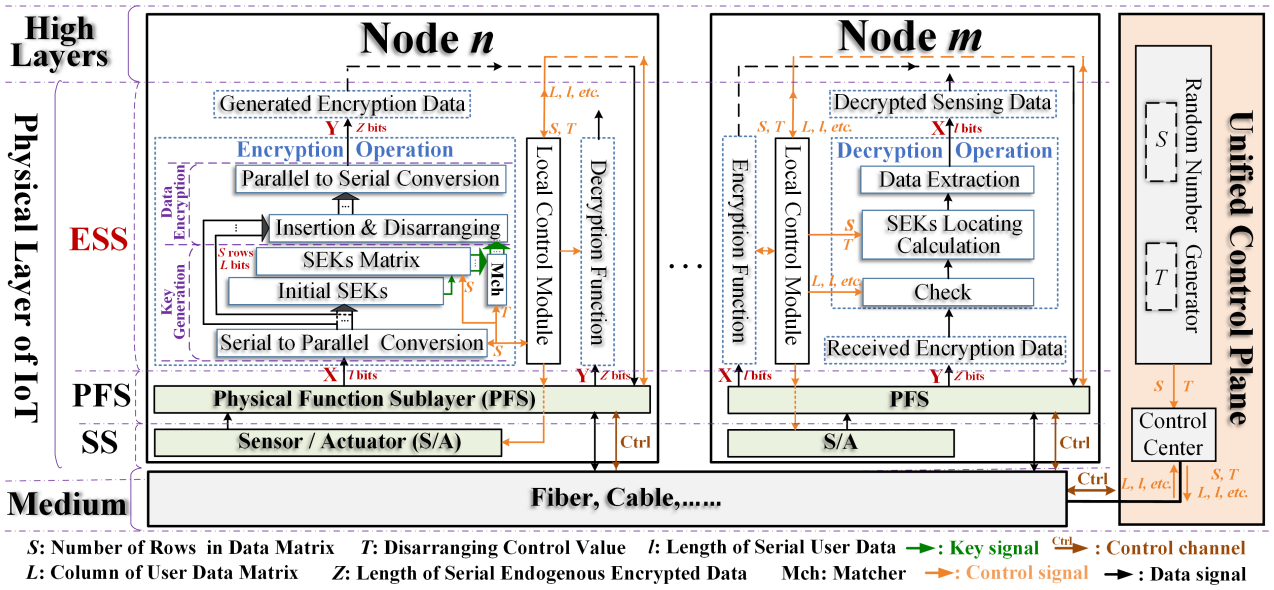


Fig. 2: SEK-based DSE scheme for the PHY-ES architecture of IoT.

represent the physical layer in Fig.1 (n, m=1, 2, …, $n\neq m$), and provide the encryption and decryption of the scheme in ESS in detail as follows, respectively, and the frameworks of PFS and SS are the same as those in Fig.1.

First of all, a unified control plane generates the random numbers S and T as the control parameters for the scheme of node n. The long serial sensing data X with a length of l bits from the SS are sliced and converted into a data matrix with S rows through the serial to parallel part, and each row in the data matrix has the same length L. By quantifying the randomness in the column space of the data matrix, the initial SEKs related to the values of L columns in the data matrix are generated in the initial SEKs part. Therefore, the SEKs matrix can be created with S rows and B columns ($B = \lfloor L/S \rfloor$).

Subsequently, according to control parameter T, the SEKs matrix needs to be inserted into the data matrix. In this way, the data matrix arrangement has been completely disarranged by inserting the SEKs matrix.

Subsequently, the endogenous encrypted sensing data Y with a length of Z bits (Z=l+L) are obtained by parallel to serial conversion. At this point, endogenous encryption of the original sensing data has been completed.

The series of parameters generated during the above encryption process (such as l, L, etc.) are directly fed back to the unified control plane and then sent to the check part at node m. Thus, encrypted sensing data Y is received and can be checked at this node. By finding the corresponding S and T, and calculating the SEK locations of Y, X can quickly and accurately decrypt from the checked Y.

III. Process, Algorithm and Verification

In order to implement the SEK-based DSE scheme for the PHY-ES architecture, this section details the process of the scheme, establishes the corresponding algorithm, and finally verifies the performance of the scheme by simulation.

A. Process of SEK-based DSE Scheme

The encryption process of the SEK-based DSE scheme is shown in Fig.3, where input port 1 inputs S and T, input port 2 inputs sensing data X, and output port outputs endogenous encrypted sensing data Y. After X is sliced and converted into a data matrix $\mathbf{X}$ with S rows and L columns in the serial to parallel part, the randomness of the column in $\mathbf{X}$ is quantified in the initial SEKs part [20]. In the matrix part, the quantification result of $\mathbf{X}$ is an SEK matrix $\mathbf{K}$ with S rows and B columns generated based on the initial SEKs. The i-th row of $\mathbf{K}$ is inserted into the corresponding row of $\mathbf{X}$, the $\mathbf{K}$ includes k_{i-1}~k_{i-B}, where i is the row order, $1 \le i \le S$. After matching $\mathbf{K}$ with T_i, in the insertion and disarranging part, $\mathbf{X}$ and $\mathbf{K}$ are disarranged according to T_i. When i=S, Y_S is obtained by combining and disarranging the sensing data x_{S1}~x_{SL} with SEKs k_{S-1}~k_{S-B} based on T_S. After the parallel to serial conversion, Y: y_1~y_Z is the output.

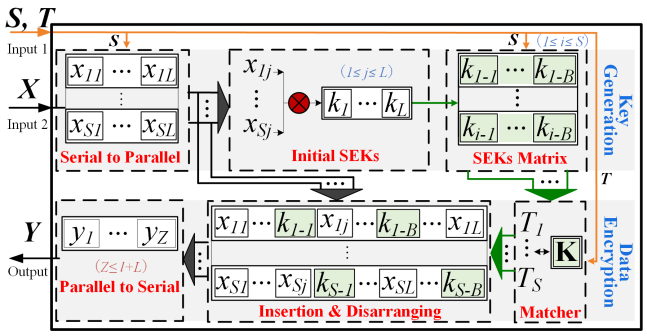


Fig. 3: Encryption process of SEK-based DSE scheme.

The decryption process of the SEK-based DSE scheme is shown in Fig.4. The input port 1 inputs the endogenous

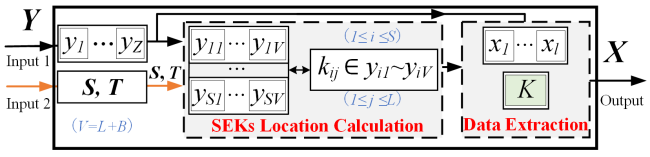


Fig. 4: Decryption process of SEK-based DSE scheme.

encrypted sensing data Y, the input port 2 inputs S and T. Theoutput port outputs the decrypted sensing data X. When Y: $y_1 \sim y_Z$ is received and checked successfully, in the SEK location calculation part, the location of SEK k_{ij} is calculated in a data matrix composed by $y_1 \sim y_Z$ based on S and $T_1 \sim T_S$. Then, in the data extraction part, the sensing data $x_1 \sim x_l$ are separated from Y, and X is the output, where $V=L+B$.

B. Algorithm of SEK-based DSE Scheme

According to the SEK-based DSE scheme, we give the corresponding algorithm as follows

$$\begin{aligned} \mathbf{Y} &= E(\mathbf{X}) \\ &= \prod_{v=1,2,3} E_v(\mathbf{X}) = E_1\{E_2[E_3(\mathbf{X})]\} \end{aligned} \tag{1}$$

where $\mathbf{X}$ with S rows and L columns is the input matrix, $\mathbf{Y}$ is the output matrix of, and E is the encryption algorithm.

According to the encryption process in Fig. 3, E can be divided into algorithms E_1, E_2, and E_3 for generating initial SEKs, creating SEKs matrix, and inserting SEKs into sensing data by disarranging, respectively. Each of the three algorithms is described in pseudocode as follow.

Algorithm $\mathbf{E}_1$: Input: $\mathbf{X}_1$=$\mathbf{X}$; Require: $\mathbf{Y}_1$

for j = 1:1:L do
  $\mathbf{E}_1(j)$ = 0;
  for i = 1:1:S do
    $\mathbf{E}_1(j)$ = *Calculate* [$\mathbf{E}_1(j)$, $\mathbf{X}_1(i,j)$];
  end for
  $\mathbf{Y}_1(j)$ = $\mathbf{E}_1(j)$;
end for
output [$\mathbf{Y}_1(1)$, …, $\mathbf{Y}_1(L)$]

where $\mathbf{X}_1$=$\mathbf{X}$ is the input matrix, $\mathbf{E}_1$ is the generation matrix of the initial serial SEKs, output matrix $\mathbf{Y}_1$ is the initial serial SEKs. The *Calculate* function quantifies the column randomness of $\mathbf{X}_1$. $\mathbf{X}_1(i, j)$ is the element of $\mathbf{X}_1$ in the i-th row and j-th column, $\mathbf{E}_1(j)$ is the j-th column of $\mathbf{E}_1$, $\mathbf{Y}_1(j)$ is the j-th element of $\mathbf{Y}_1$.

Algorithm $\mathbf{E}_2$: Input: $\mathbf{X}_2$=$\mathbf{Y}_1$; Require: $\mathbf{K}$ = $\mathbf{Y}_2$

initial $B = \lfloor L/S \rfloor$;
for i = 1:1:S do
  $\mathbf{Y}_2(i) = \mathbf{X}_2 \cdot \mathbf{E}_2(i) = \mathbf{Y}_1 \cdot (\mathbf{O}_1, \ldots, \mathbf{I}_i, \ldots, \mathbf{O}_S)'$;
end for
output $\mathbf{K} = \mathbf{Y}_2 = \begin{bmatrix} \mathbf{Y}_2(1) \\ \vdots \\ \mathbf{Y}_2(S) \end{bmatrix}$

where $\mathbf{X}_2$=$\mathbf{Y}_1$ is the input matrix, $\mathbf{Y}_2$ is the output matrix with S rows and B columns, $\mathbf{Y}_2(i)$ is the i-th row of $\mathbf{Y}_2$, $\mathbf{E}_2$ is the generation matrix of the SEKs matrix and consists of S small matrices with only one small matrix is the identity matrix $\mathbf{I}$ and the others are all zero matrix $\mathbf{O}$. $\mathbf{K}$ is the SEK matrix.

In X_3 is the input matrix consisting of the $\mathbf{X}$ and the $\mathbf{K}$, $\mathbf{Y}_3$ is the output matrix. The function $E_3\{\mathbf{X}_3, i, T_i\}$ represents that the i-th row of $\mathbf{K}$ is inserted into the i-th row of $\mathbf{X}$ and multiplied by 2^{Ti}, so as to disarrange the i-th row of $\mathbf{X}$ and $\mathbf{K}$.

Algorithm $\mathbf{E}_3$: Input: $\mathbf{X}_3$=$\mathbf{X}$ and $\mathbf{K}$; Require: $\mathbf{Y}$=$\mathbf{Y}_3$

initial $T = (T_1, \ldots, T_S)$;
for i = 1:1:S do
  $\mathbf{Y}_3(i) = E_3\ [\mathbf{X}_3, i, T_i]$;
end for
output $\mathbf{Y} = \mathbf{Y}_3 = \begin{bmatrix} \mathbf{Y}_3(1) \\ \vdots \\ \mathbf{Y}_3(S) \end{bmatrix}$

And the algorithm for decryption process is shown below.

$$D(\mathbf{Y}) = D[E(\mathbf{X})] = \mathbf{X} \tag{2}$$

where D is the decryption algorithm that is described as follows.

We define $\mathbf{Y}(i)$ as the i-th part of $\mathbf{Y}$, $\mathbf{X}(i)$ is the i-th row of $\mathbf{X}$, the $D\{\mathbf{Y}(i)\}$ is responsible for resetting $\mathbf{Y}(i)$ and extracting $\mathbf{X}(i)$ form it, composed by an $\mathbf{I}$ and an $\mathbf{O}$.

Algorithm D: Input: $\mathbf{Y}$; Require: $\mathbf{X}$

initial $V = L + B$;
for i = 1:1:S do
  $\mathbf{Y}(i)$ = [$Y_{1+V\cdot(i-1)}$, …, $Y_{V\cdot i}$];
  $\mathbf{X}(i)$ = D[$\mathbf{Y}(i)$] = [$\mathbf{Y}(i)\cdot 2^{-Ti}$] · ($\mathbf{I}$ $\mathbf{O}$)$_i$';
end for
output $\mathbf{X} = \begin{bmatrix} \mathbf{X}(1) \\ \vdots \\ \mathbf{X}(S) \end{bmatrix}$

C. Performance Evaluation Method

To evaluate the performance of the SEK-based DSE scheme, we determine a special parameter as DLC, which represents the duration time T_{DLC} of sensing data confidentiality at the physical layer of IoT. T_{DLC} is defined as following

$$T_{DLC} = T_e + T_d + T_t + T_a \tag{3}$$

where T_e and T_d are the processing time spent in the encryption module and decryption modules, respectively. T_t is the transmitting time in medium. T_a is the additional time, such as the modulation, demodulation, encoding, queuing, and so on.

$$\begin{cases} t_e = T_e/l \\ t_d = T_d/Z \\ n_e = Z/l = 1 + L/l \end{cases} \tag{4}$$

Meanwhile, we determine another special parameter as AC, including t_e, t_d, and n_e, where t_e and t_d are the average time required for encrypting and decrypting each bit of sensing data, respectively, n_e is the average bits required for encrypting each bit of sensing data. It is obvious that the smaller the DLC

is and the lower the AC is, the better the performance of the SEK-based DSE scheme for the PHY-ES architecture is.

The time of the illegal node forcibly deciphers encrypted sensing data is defined as T_i, and represented by the combination of T_e, T_d, and coefficients ϕ and γ.

$$T_i = (\frac{L^*}{2} - 1)^2 \cdot S^* \cdot T^* \times (\phi \cdot T_e + \gamma \cdot T_d) \quad (5)$$

where L^* is length of the intercepted encrypted sensing data, S^* and T^* are the values of S and T guessed by external illegal nodes, respectively. Then the deciphering probability η as follows

$$\eta = T_d/T_i = \frac{1}{(\frac{L^*}{2} - 1)^2 \cdot S^* \cdot T^* \times (\phi \cdot \frac{T_e}{T_d} + \gamma)} \quad (6)$$

where η is the ratio of T_i to T_d for the same encrypted sensing data. Therefore, the greater the difference between T_e and T_d is, and the longer L is, the larger the value range of S and T is, then the smaller the η is and the higher the security of the encrypted sensing data is.

All in all, in addition to DLC, AC, and η mentioned above, the SEK-based DSE scheme can also be evaluated from other different perspectives, such as energy consumption, algorithm complexity, and so on. And the IoT physical layer has to face the similar security threats as those existing in the current Internet, including eavesdropping, interference, sabotage, etc. The SEK-based DSE scheme has strong defensive capabilities when dealing with eavesdropping threats, but it is still necessary to conduct research on corresponding defense mechanisms against other attacks to ensure the PHY-ES of IoT.

D. Simulation of SEK-based DSE Scheme

Based on the process, algorithm, and method of SEK-based DSE scheme built above, we simulate the scheme in MATLAB, and analyze and verify the changes of the DLC and AC with different sensing data lengths. And the system time of MATLAB is unified as the unit time (u.t).

We simulate the DLC for the scheme draw the curves of T_{e-s}, T_{d-s}, and T_{DLC-s} as L increases from 1×10^3 bits to 10×10^3 bits with S=10, S=50, and S=100, as shown in Fig.5, so as to explore the suitable length of slicing. In Fig.5, T_{e-s} and T_{d-s} are defined as the processing times of encryption and decryption in simulations, respectively, and T_{DLC-s} is the duration time of the sensing data encrypted by the SEKs at the physical layer of IoT in simulations.

In Fig.5 (a), by comparing the curves with the same color, T_{e-s} is larger than T_{d-s}, e.g., blue curves, when S=100 and L=10×10^3 bits, T_{e-s}=66.3 u.t > T_{d-s}=25.5 u.t. When L is fixed, regardless of the value of S, the gap between T_{e-s} and T_{d-s} becomes larger with the increase of S. For example, when L=10×10^3 bits, the value of $\Delta(T_{e-s}\text{-}T_{d-s})$ increases by approximately 89.7 times as S increases from 10 to 100. Since the time complexity of the encryption algorithm is nonlinear, while the decryption algorithm is linear, T_{e-s} is significantly larger than T_{d-s}, and $\Delta(T_{e-s}\text{-}T_{d-s})$ widens, as the total amount of sensing data increases.

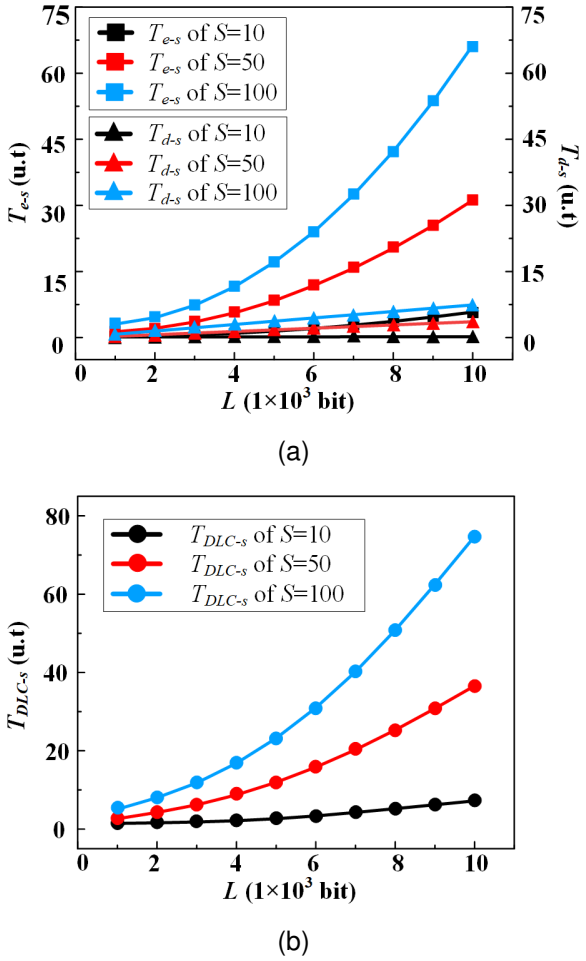


Fig. 5: Simulation results of how (a) T_{e-s}, T_{d-s}, and (b) T_{DLC-s} vary with L.

In Fig.5 (b), assuming T_t+T_a =1 u.t in simulations, when S is constant, as L increases, T_{DLC-s} increases, and the larger S is, the faster T_{DLC-s} increases. Although, it is noted that the curve of T_{DLC-s} is similar to that of T_{e-s} with the same S in Fig. 5 (a), they are not completely consistent.

Then, we carry out a simulation of the AC for the scheme, and draw the curves about t_{e-s}, t_{d-s}, and n_{e-s} as L increases from 1×10^3 bits to 10×10^3 bits under the conditions of S=10, S=50, and S=100, as shown in Fig.6, where t_{e-s} and t_{d-s} are the average times required for encrypting and decrypting each bit of sensing data in the simulations, respectively, and n_{e-s} is the average number of bits required for encrypting each bit of sensing data in the simulations.

In Fig.6 (a), when S is fixed, the trends of curves t_{e-s} and t_{d-s} are opposite to those of T_{e-s} and T_{d-s}, respectively. With an increase in L, t_{e-s} and t_{d-s} decrease, and both reach the minimum value at approximately L=8×10^3 bits. When S=100, the minimum values of t_{e-s} and t_{d-s} are 0.678×10^{-4} u.t and 0.235×10^{-4} u.t, respectively, whereas when S=10, the minimum values of t_{e-s} and t_{d-s} are 0.536×10^{-4} u.t, and 0.109×10^{-4} u.t, respectively.

In Fig.6 (b), when S is fixed, with the increase of L, n_{e-s} decreases during L=1×10^3~4×10^3 bits, and then becomes stable during L=8×10^3~10×10^3 bits. Obviously, n_{e-s} starts approaching the minimum value around L=8×10^3 bits under

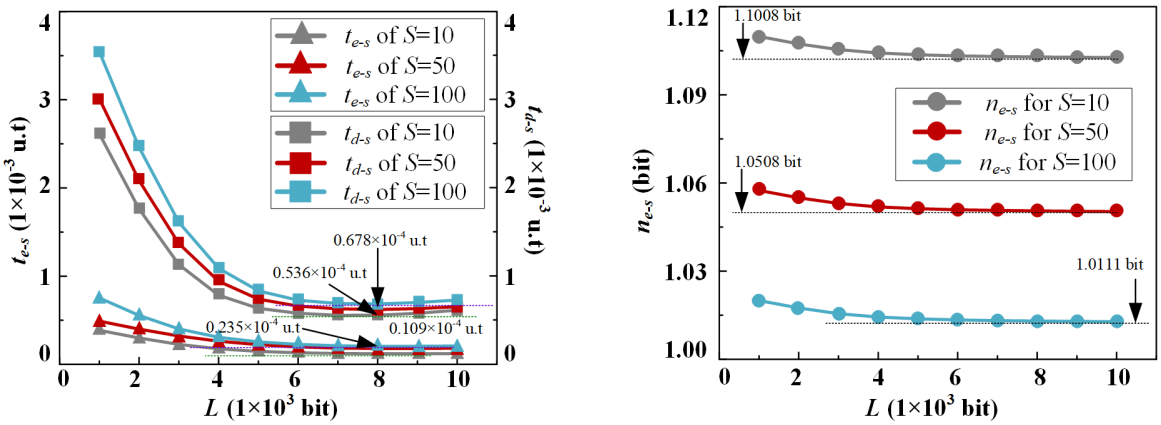


Fig. 6: Simulation results of (a) t_{e-s}, t_{d-s}, and (b) n_{e-s} vary with L.

all conditions, and the minimum values of n_{e-s} for S=10 and S=100 are 1.1008 and 1.0111 bits, respectively. As can be observed from the figure, the less the slicing length of the sensing data, the smaller the DLC is and the better the sensing data confidentiality, but the higher the AC.

IV. Experiments and Discussions

According to the above process, algorithm, and simulation of the scheme proposed here, for further verification, we need to explore a simplified experimental approach, build an experimental system at the lab, and discuss the experimental results. Meanwhile, we compare the experimental results with similar reported schemes.

A. Experimental Scheme

We design an experimental platform for the SEK-based DSE scheme suited for the PHY-ES architecture as shown in Fig.7, in which two physical layer nodes with a small form pluggable (SFP) interface each are connected by using a section of optical fiber. Node 1 encrypts the sensing data sent from the sensing database, transmits the encrypted sensing data to node 2 and the server computer through optical fiber and a universal serial bus (USB) interface respectively. After decrypting the encrypted sensing data at node 2, it is sent to the server computer through a USB interface in the node. To simplify the experimental system, the computer has both control signal transmission and encrypted/decrypted sensing data reception functions, and is directly connected to two nodes through USB interfaces, by using the cable. Thus, the control parameters S and T are sent to the two nodes directly. At the same time, the sensing data at the bottom left in node 1 can be produced by the random number generator. During the testing process, we mainly focus on verifying the SEKs generation and both encryption and decryption functions.

According to the approach above, we set up an experimental system with two physical layer nodes for SEK-based DSE scheme, implemented by using a FBGA (Xilinx KC705) board, as shown in Fig.8 in the lab. Two FPGA boards are connected with each other through a single mode fiber G.652D with 10 kilometers and SFP optical transceivers. The server computer and monitor are directly connected to the two boards through USB interfaces and cable, so that the encrypted sensing data Y and decrypted sensing data X can be displayed on the monitor.

Figs.9 (a) and (b) illustrate the flow chart for data processing of encryption and decryption of the SEK-based DSE scheme, on which the software is developed by the Vivado and inserted in two nodes, respectively. To observe the processing time of encryption and decryption at the debug window of an integrated logic analyzer, respectively, a counter is both set

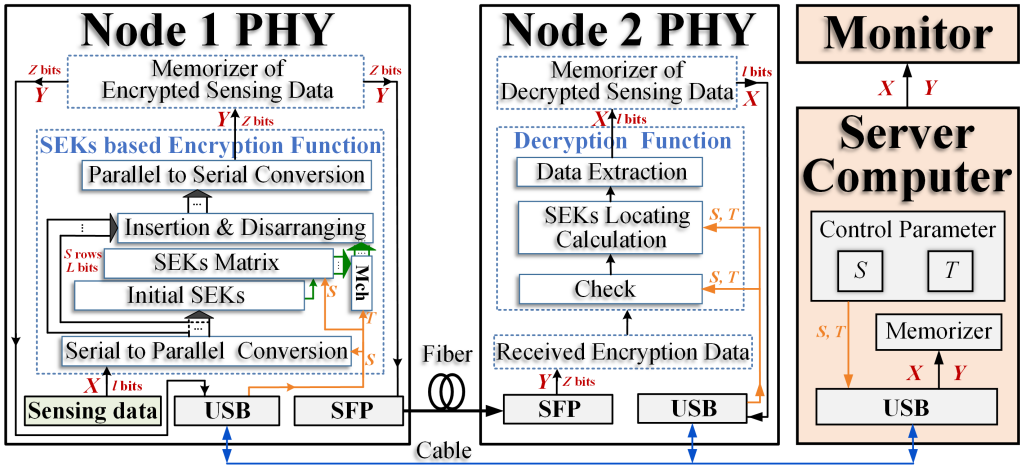


Fig. 7: Experimental platform for the SEK-based DSE scheme suited for the proposed PHY-ES architecture.

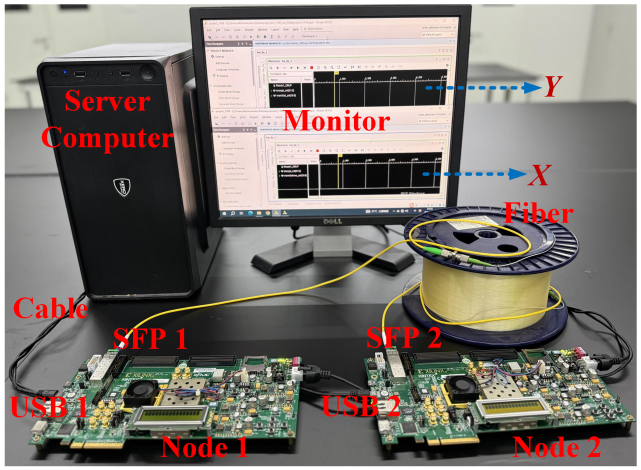


Fig. 8: Experimental system of the SEK-based DSE scheme built in our lab.

and turned on at the start of encryption and decryption, and is both stopped and outputted the counter results at the end.

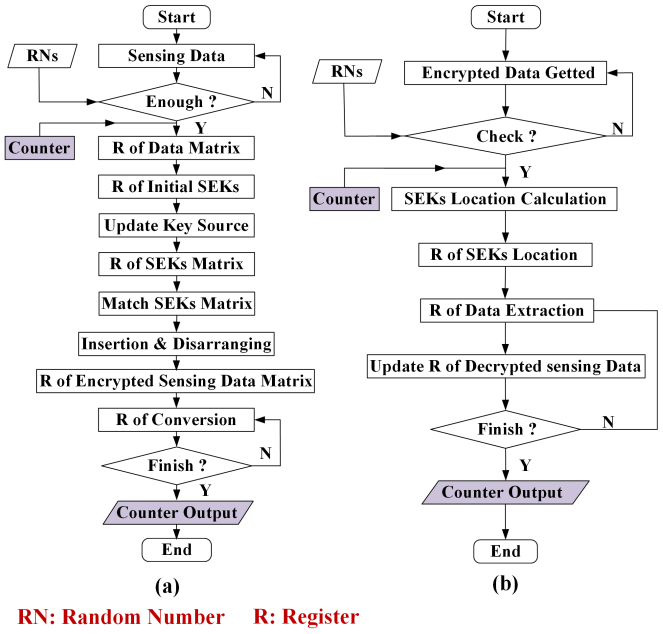


Fig. 9: Flow chart for data processing about (a) encryption and (b) decryption of SEK-based DSE scheme on FPGA.

The experiment results of nodes 1 and 2 are shown in Figs.10 (a) and (b), where Ready1_OBUF=1 indicates that the encryption or decryption is in progress, encrypt_cnt and decrypt_cnt indicate T_e and T_d, respectively. Due to the total number limitation of the observable bits in waveform of debug window, the encrypted sensing data and the decrypted sensing data cannot be observed, we estimate the ne roughly by counting the number of "1" codes in data, based on the law of large numbers. The memGet_cnt and memGetnew_cnt are used to indicate the number of "1" codes in encrypted sensing data and the decrypted sensing data, respectively.

B. Results and Discussions

During the testing, we repeat two hundred times and average the testing data to draw the experimental results for each one.

Figs.11 (a) and (b) depict how T_{e-e} and T_{d-e} vary with L under different values of S, and compare the obervations with the simulated ones for T_{e-s} and T_{d-s}, respectively. T_{e-e} and T_{d-e} are defined as the processing time for encryption and decryption on nodes 1 and 2, respectively. If L and S are constant, T_{e-e} is always greater than T_{d-e}. And only S is constant, both T_{e-e} and T_{d-e} increase with L, but the rate of increase of T_{e-e} is obviously faster than that of T_{d-e}. When only L is fixed, the larger S is, the larger T_{e-e} and T_{d-e} are.

The above experimental results are almost consistent with the simulation results shown by the solid line with light blue, light red and light black in Figs.11 (a) and (b). However, there are some differences between T_{e-e} and T_{e-s}, as well as T_{d-e} and T_{d-s}, which are caused by the delay deviation stemming from FPGA logic circuit instability, power instability, register reading, and so on.

Fig.12 shows T_{DCL-e} varies with L under the conditions of S=10, S=50, and S=100, and compares T_{DCL-e} with the simulation values, where T_{DCL-e} is the duration of the sensing data encrypted by SEK at the physical layer of IoT in the experiments. Meanwhile, we assume that the transmit time T_t and additional time T_a are calculated according to the length of fiber, the number of bits transmitted, as well as the transmission rate of SFP during testing.

As can be observed from Fig.12, the value of T_{DCL-e} is similar to T_{DCL-s}, but the values of T_{DCL-e} values are always slightly larger than the simulated ones with values of S and L. The larger S and L are, the larger the difference between T_{DCL-e} and T_{DCL-s} is. This is because the transmission time T_a for encrypted sensing data is constant in simulation, but it is a variable in experiment and varies with total amount of transmitted data.

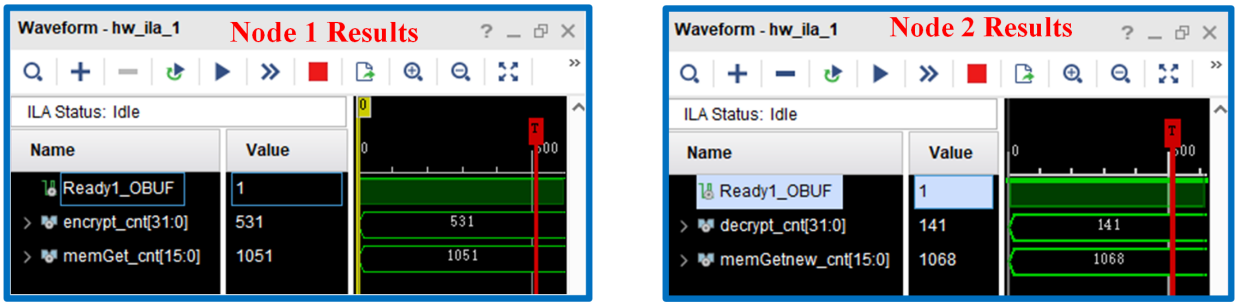
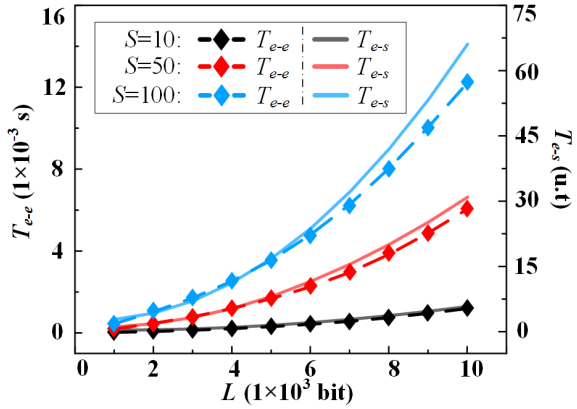
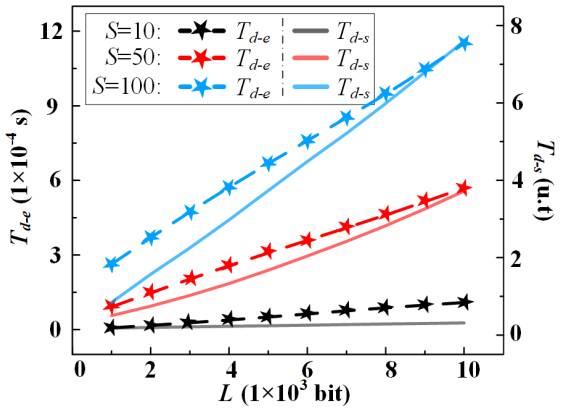


Fig. 10: Experiment results of (a) node 1 and (b) node 2.

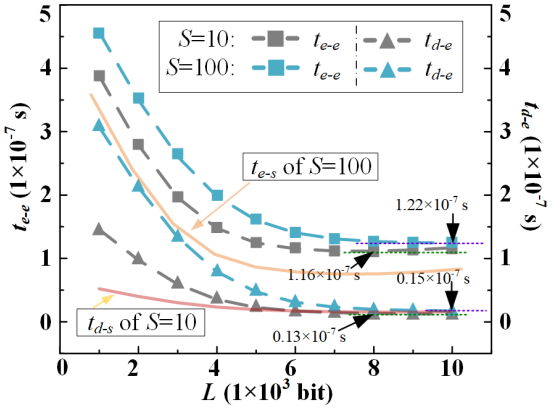


(a)

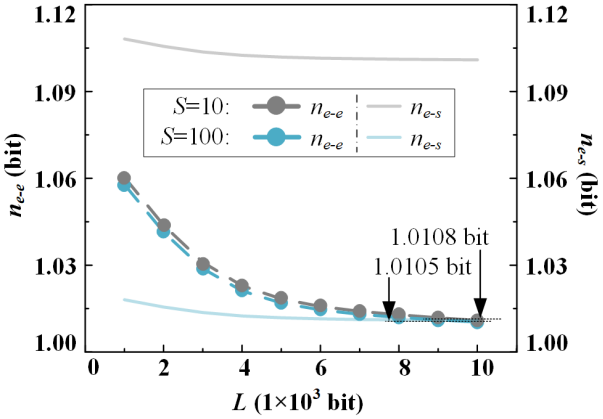


(b)

Fig. 11: Experimental results of (a) T_{e-e} and (b) T_{d-e}, change with L, and compared with the simulation ones for T_{e-s} and T_{d-s}, respectively.



(a)



(b)

Fig. 13: Experimental results of (a) t_{e-e} and (b) n_{e-e}, change with L, and compared with the simulation ones for t_{e-s} and n_{e-s}, respectively.

Fig.13 (a) depicts t_{e-e} and t_{d-e} vary with L, and the comparison with the simulation ones for t_{e-s} and t_{d-s}, where t_{e-e} and t_{d-e} are the average time required for encrypting and decrypting each bit of sensing data in experiments, respectively. When L is fixed, the larger S is, the larger t_{e-e} and t_{d-e} are. When S is fixed, as L increases, t_{e-e} and t_{d-e} gradually tend to the minimum value, which are opposite to the change trend of T_{e-e} and T_{d-e}, respectively. When S=100, t_{e-e} and t_{d-e} approach the minimum values of 1.22×10^{-7} s and 0.15×10^{-7} s, around L=10×10^3 bits, respectively. However, when S=10, t_{e-e} and t_{d-e} approach the minimum values of 1.16×10^{-7} s and 0.13×10^{-7} s, around L=8×10^3 bits, respectively. And the experimental results have some differences with the simulations shown by the orange and red solid lines, which are caused by the delay deviation of the FPGA board, the transmission hysteresis of the control signal during test, etc.

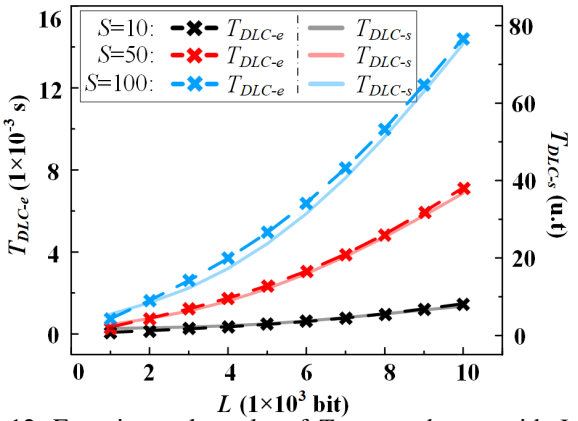


Fig. 12: Experimental results of T_{DCL-e} change with L, and compared with the simulation ones for T_{DCL-s}.

Fig.13 (b) plots n_{e-e} based on the assumption that the codes for bits "1" and "0" are the same in one sensing data bit, and compared with the n_{e-s}, where n_{e-e} is the average number of bits required for encrypting each bit of the sensing data in the experiments. As can be seen from the figure, n_{e-e} decreases as L increases, and around L=8×10^3 bits, it tends to approach the minimum value under all sensing data lengths, which is almost same as the simulation results in Fig.6 (b). However, there are some differences between the experimental and simulated results shown by the solid line with lighter color for the case of S=10 with all values of L and the case of S=100 with L=1×10^3 bits~6×10^3 bits. Since the above assumption is based on the law of large numbers, and the longer the length of the sensing data is, the closer the experimental results to their simulated counterparts are.

C. Performance Comparisons

Among many physical layer encryption schemes for IoT, deep learning-based schemes have better performance than other ones. Therefore, this section compares the performance of the SEK-based DSE scheme with the key generation neural network (KGNet) presented in [16] and the bidirectional convergence feature learning (BCFL) network presented in [17]. Firstly, the biggest difference between the proposed scheme in this paper and the latter two is that the former uses SEKs, while the latter two require external key sources.

Next, we compare the performance of three schemes under different total amounts of sensing data l, where the execution time and key generation amount in per unit time of both [16] and [17] are similar to the T_{e-e} and n_{e-e} of the experimental results of our scheme.

Fig.14 compares the T_{e-e} results of our scheme with those of the KGNet and BCFL when l=1×10^3, 50×10^3, and 100×10^3 bits, respectively. It is obvious that T_{e-e} of our scheme is better than those of the KGNet and BCFL, and the larger the l, the greater the T_{e-e} difference of the three schemes. In particularly, when l=100×10^3 bits (purple column), the T_{e-e} of our scheme reduces by 75.22% and 18.65%, compared with the KGNet and BCFL, respectively.

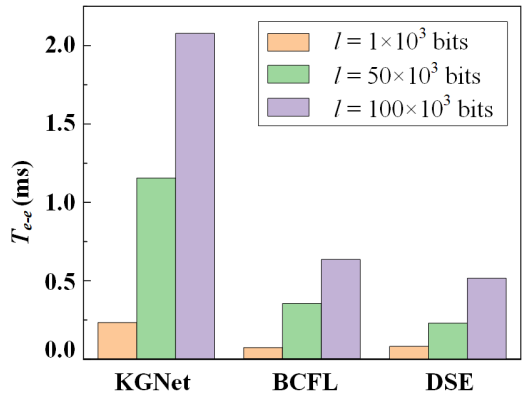


Fig. 14: T_{e-e} comparison of our scheme with KGNet and BCFL.

The reason why DSE performs better in Fig.14 is that the KGNet and BCFL are both traditional encryption schemes with classical external key source, while the DSE scheme can generate SKEs and encrypt sensing data inside the IoT physical layer system. It is future means that the novel idea of endogenous key source proposed in this paper can effectively improve the encryption performance of massive sensing data at the physical layer of IoT.

Fig.15 compares n_{e-e} of our scheme with those of the KGNet and BCFL when l=1×10^3, 50×10^3, and 100×10^3 bits. When l is small, the n_{e-e} for our scheme is approximately equal to that for KGNet, and both are greater than that for BCFL. When l is larger, e.g. l=100×10^3 bits (purple column), compared to KGNet and BCFL, our scheme performs better and reduces by 24.13% and 47.2% for n_{e-e}, respectively. As l increases, the n_{e-e} values of the three schemes tend to their respective minimum values, respectively. The reason of DSE performs better than KGNet and BCFL is same as above.

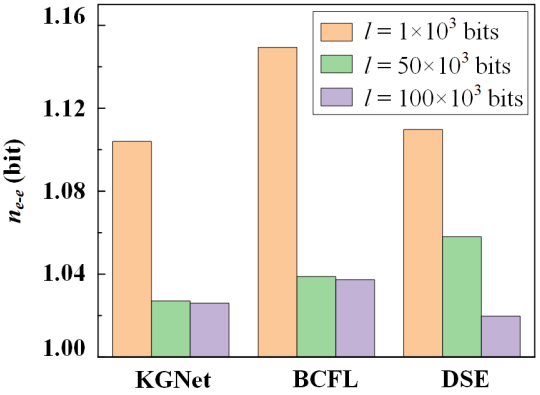


Fig. 15: n_{e-e} comparison of our scheme with KGNet and BCFL.

To summarize, we conclude that the SEK-based DSE scheme for the PHY-ES architecture of IoT has high security and low overhead without needing any external key source. Compared with the KGNet, T_{e-e} and n_{e-e} of our scheme are reduced by 75.22% and 24.13%, respectively, while the reeducations are 18.65% and 47.2% compared with the BCFL, respectively.

V. Conclusion

In this paper a novel PHY-ES architecture and an SEK-based DSE scheme suited for IoT were proposed. The motivation of this architecture was to provide both endogenous encryption and decryption functions for massive amounts of heterogeneous sensing data in the physical layer, especially for unique scenes of IoT, where the sensing data traffic in the uplink is far larger than the one of the downlinks. The scheme can generate SEKs by quantifying the randomness of sensing data without any external key source, encrypt and decrypt the sensing data directly in the physical layer. After the detailed process of the scheme is given, a corresponding algorithm for the scheme was established and its simulation results were analyzed. A simplified experiment platform was constructed, on which the performance of the SEK-based DSE scheme for PHY-ES architecture was demonstrated to be viable and effective for protecting the sensing data, and can reduce the DLC and AC on average by about 42% and 35%, compared with other schemes, respectively. All in all, the PHY-ES architecture and the SEK-based DSE scheme proposed in this paper provide a unique and advantageous approach for accessing to massive heterogeneous sensing data securely in IoT.

Currently, due to the diverse functions and types of sensors and actuators, the actually deployed IoT will face the challenges, such as multi-source heterogeneous sensing data access, unstable uplink channels, eavesdropping attacks, etc. Although the SEK-based DSE scheme can adapt to the relatively complex conditions of IoT, with the rapid development of IoT technologies in application, there are still some research works to be carried out in security analysis, practical deployment, scalability, and energy consumption of SEK-based DSE scheme. Firstly, by combining the artificial intelligence algorithms to strengthen the preprocessing of sensing data, the security of SEK-based DSE scheme can be improved. Secondly,

the efficient sensing data access and aggregation schemes should be considered with the SEK-based DSE scheme to enhance its performance in complex network environments. Finally, we should expand the evaluation parameters, such as energy consumption, algorithm complexity, etc., and analyze the SEK-based DSE scheme from more perspectives.

REFERENCES

[1] A. Hazra *et al.*, "Fog computing for next-generation Internet of Things: Fundamental, state-of-the-art and research challenges," *Computer Sci. Rev.*, vol. 48, May 2023.

[2] J. Lin *et al.*, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," *IEEE Internet Things*, vol. 4, no. 5, pp. 1125-1142, Oct. 2017.

[3] S. Baker *et al.*, "Artificial Intelligence of Things for Smarter Healthcare: A Survey of Advancements, Challenges, and Opportunities," *IEEE Commun. Surv. Tut.*, vol. 25, no. 2, pp. 1261-1293, Jun. 2023.

[4] J. Ahmad *et al.*, "Machine learning and blockchain technologies for cybersecurity in connected vehicles," *Wires. Data Min. Knowl.*, vol. 14, no. 1, Sep. 2023.

[5] Y. F. Han *et al.*, " Reputation-aware rate maximization for cross-media cooperative transmission in smart ocean IoT," *IEEE Internet Things*, vol. 10, no. 20, pp. 19062-19074, Nov. 2023.

[6] Overview of the Internet of Things, ITU-T Y.4000 Recommendation, 2012.

[7] Functional framework and capabilities of the Internet of Things, ITU-T Y.4401 Recommendation, 2015.

[8] N. Abbas *et al.*, "Mobile Edge Computing: A Survey," *IEEE Internet Things*, vol. 5, no. 1, pp. 450-465, Feb. 2018.

[9] Sensor control networks and related applications in a next generation network environment, ITU-T Y.4250 Recommendation, 2013.

[10] IEEE Standard for broadband over power line networks: medium access control and physical layer specifications, IEEE Std 1901TM-2020 (Revision of IEEE Std 1901-2010), 2021.

[11] Y. D. Fu *et al.*, "High-speed optical secure communication with an external noise source and an internal time-delayed feedback loop," *Photonics Res.*, vol. 7, no. 11, pp. 1306-1313. Nov. 2019.

[12] J. B. Perazzone *et al.*, "Artificial Noise-Aided MIMO Physical Layer Authentication with Imperfect CSI," *IEEE T. Inf. Foren. Sec.*, vol. 16, pp. 2173-2185, Jan. 2021.

[13] X. F. Tang *et al.*, "A Physical Layer Security-Enhanced Scheme in CO-OFDM System Based on CIJS Encryption and 3D-LSCM Chaos," *J. Lightwave Technol.*, vol. 40, no. 12, pp. 3567-3575, Jun. 2022.

[14] N. Jiang *et al.*, "Physical secure optical communication based on private chaotic spectral phase encryption/decryption," *Opt. Lett.*, vol. 44, no. 7, pp. 1536-1539, Apr. 2019.

[15] Y. K. Chen *et al.*, "Security Analysis of QAM Quantum-Noise Randomized Cipher System," *IEEE Photonics J.*, vol. 12, no. 4, pp. 1-14, Aug. 2020.

[16] X. W. Zhang *et al.*, " Deep-Learning-Based Physical-Layer Secret Key Generation for FDD Systems," *IEEE Internet Things*, vol. 9, no. 8, pp. 6081-6094, Apr. 2022.

[17] Y. R. Chen *et al.*, "Physical-Layer Secret Key Generation Based on Bidirectional Convergence Feature Learning Convolutional Network," *IEEE Internet Things*, vol. 10, no. 16, pp. 14864-14855, Aug. 2023.

[18] IEEE Standard for Ethernet, IEEE Std 802.3-2022 (Revision of IEEE Std 802.3-2018), 2022.

[19] IEEE/ISO/IEC Telecommunications and exchange between information technology systems – Requirements for local and metropolitan area networks – Part 3: Standard for Ethernet AMENDMENT 4: Physical layers and management parameters for 50 Gb/s,200 Gb/s, and 400 Gb/s operation over single-mode fiber, IEEE/ISO/IEC 8802-3:2021/Amd 4-2021, 2021.

[20] X. Ye *et al.*, "A Key Generation Scheme from Sensing Data for IoT Security," in *Proc. IEEE Conf. Commun. Net. Secy. (CNS)*, Orlando, USA, Oct. 2023, pp. 1-2.

Xiaokai Ye received the B.S. degree from Hainan University, Haikou, China, in July 2017. He is currently working toward the Ph.D. degree in electronic engineering with Southeast University, Nanjing, China. His research focuses on the physical layer security of IoT.

Tao Lv received the B.S. degree and the Ph.D degree in electronic engineering in 2016 and 2024 from Southeast University, Nanjing, China, respectively. His research focuses on optical sensing and long-haul optical communication.

Kun Huang received a PhD in Electronic Engineering from Southeast University in Nanjing, China in June 2024. He is working at Nari Group in Nanjing, China. His research focuses on sensor network access technology.

Jinhui Li received Ph.D. degrees in electronic engineering from the Southeast University, Nanjing, China, in 2001. After working for over 20 years in Fortune Global 500 companies, she joined Nanjing Xiguang Research Institute. Her research areas include signal processing, communication, the IoT.

Xuekang Shan received the PhD degree in optical fiber communications from University of Essex, UK, in 1995. He held senior technical positions in Fortune Global 500 companies for over 20 years. He has been a technical consultant of Nanjing Xiguang Research Institute since 2017. His research interests include optical fiber communications.

Wei Xiang (Senior Member, IEEE) received the B.Eng. and M.Eng. degrees in electronic engineer ing from the University of Electronic Science and Technology of China, Chengdu, China, in 1997 and 2000, respectively, and the Ph.D. degree in telecom munications engineering from the University of South Australia, Adelaide, SA, Australia, in 2004. He is currently the Cisco Research Chair of AI and IoT and the Director of the Cisco-La Trobe Centre for AI and IoT, La Trobe University, Melbourne, VIC, Australia.

Xiaohan Sun is currently a Professor with the Scholl of Electronics Science Engineering and the Director of the National Research Center for Optical Sensing/Communications Integrated Networking, Southeast University, Nanjing, China. Her research interests include optical communications and sensing, the IoT.

A Physical Layer Endogenous Security Architecture with Dynamic Slicing Encryption for IoT

Xiaokai Ye, Tao Lv, Kun Huang, Jinhui Li, Xuekang Shan, Wei Xiang*, and Xiaohan Sun*

***Abstract*—We propose a novel physical layer endogenous security (PHY-ES) architecture with a dynamic slicing encryption (DSE) scheme for the physical layer of Internet of Things (IoT) systems. The proposed architecture not only supports the functions of the traditional Ethernet physical layer, but also provides both endogenous encryption and decryption functions for sensing data, based on sensing endogenous keys (SEKs). A SEK-based DSE scheme is also proposed, where the SEKs are generated by quantifying the randomness of the sensing data, without needing any external key sources, which can directly encrypt the sensing data in the physical layer. Based on the above, we present the algorithm for the scheme, and give its performance evaluation method with parameters of data life cycle (DLC), average cost (AC) and deciphering probability. The simulation results for the changes in the DLC and AC are obtained under different sensing data lengths. Finally, we build an experimental platform to validate the scheme by setting up an experimental system with two nodes at the lab. The testing results show that the scheme adapts to the PHY-ES architecture with high security and low overhead performance, and the suitable slicing length is approximately L=8×10^3 bits, which are almost consistent with the simulations. Compared with other schemes, the SEK-based DSE scheme can reduce the DLC and AC by about 42% and 35% on average, respectively. The architecture and the scheme proposed in this paper provide a unique and advantageous approach for secure access to massive heterogeneous sensing data in the physical layer of IoT.**

***Index Terms*—Internet of Things (IoT), physical layer endogenous security (PHY-ES), sensing endogenous keys (SEKs), dynamic slicing encryption (DSE).**

I. Introduction

INTERNET of Things (IoT), as one solution capable with the advantages of carrying a large number of users, is widely used in medical, industry, urban construction, and other fields [1, 2]. With the development of new IoT applications, such as mini-grid, smarter healthcare, autonomous vehicles, smart ocean, etc., an increasing number of sensors and actuators with different types and levels installed in the physical layer of IoT [3–5]. Although IoT has been using the traditional Ethernet architecture and forming similar network protocols and standards [6, 7], the difference is that the sensing data traffic in the uplink channels of IoT is far greater than the one in current communication access networks [8]. This is because a large number of physical devices and modules are placed in the physical layer, the requirements of timely aggregation, processing, conversion, and transmission of sensing data are needed. The authors of [9] and [10] respectively proposed protocols enabling sensors and actuators by controller and physical layer convergence with a special data frame format, to connect sensing data to the access nodes in an orderly and reliable manner. However, the above schemes or protocols based on the traditional architecture lack an independent security function layout and corresponding transmission control channels, and the current physical layer of IoT cannot secure the sensing data traffic of the uplink channels. Therefore, it is necessary to re-plan and re-construct the physical layer architecture of the IoT.

Meanwhile, how to protect the security of massive uplink sensing data produced at the physical layer of IoT is also important. Currently, many schemes for key generation and encryption in the physical layer have been proposed. Some schemes have been proposed to generate keys from external noise sources, which encrypt a data signal into a data noise signal and transmit it with a time difference with a pure noise signal in the channels [11, 12]. Meanwhile, some schemes using different chaotic systems to generate keys have also been presented, which encrypt the original data signals into noise-like signals for transmission [13, 14]. Moreover, a scheme has been proposed to mark the signal level by utilizing the quantum-noise of the quantum system as keys, which encrypts the data signal by hiding it in the noise [15]. Other than the above physical layer key generation and encryption schemes to ensure data security by improving the anti-interception of data signals in the transmission medium, the artificial intelligence and machine learning provide novel methods for securing the sensing data traffic [16, 17]. However, these proposals not only increase the instability of the physical layer of IoT, due to that fact that external key source systems are vulnerable to external interference, such as temperature and vibration, but also increase the complexity and overhead of the physical layer of IoT, attributed to the fact that all keys need to be synchronized between the source nodes and destination nodes.

To the best of the authors' knowledge, there exist no reports of a solution that combines suitable physical layer architectures and security functions without using external key source systems for IoT sensing data in the physical layer. Therefore, we propose a novel physical layer endogenous security (PHY-ES) architecture with sensing endogenous keys (SEKs) based dynamic slicing encryption (DSE) scheme for

This work was supported by the Fundamental Research Funds for the Central Universities of China under Grant no. 2242023k30014 and no. 2242024k30048, and the National Natural Science Foundation of China under Grant no. 61271206. (Corresponding authors: Xiaohan Sun; Wei Xiang)

Xiaokai Ye, Tao Lv, Kun Huang, and Xiaohan Sun are with the National Research Center for Optical Sensing/communications Integrated Networking, Southeast University, Nanjing 210096, China.

Wei Xiang is with the School of Computing, Engineering and Mathematical Sciences, La Trobe University, Melbourne, VIC 3086, Australia.

Jinhui Li and Xuekang Shan are with the Nanjing Xiguang Research Institute for Information Technology, Nanjing 210012, China.

IoT, not only supports basic physical layer functions, but also provides both endogenous encryption and decryption functions for sensing data. The security functions can be realized in the scheme with high security and low overhead, and verified by both simulations and experiments.

In a nutshell, the main contributions can be summarized as follows.

1) *PHY-ES Architecture Providing both Endogenous Encryption and Decryption Functions*: Re-plan and re-construct the physical layer architecture of IoT based on the compatibility with traditional Ethernet physical layer architecture. We design an endogenous security sublayer (ESS) to realize both endogenous encryption and decryption, divide three data links for encrypted sensing data, decrypted receiving data, and send data, as well as an independent transmission channel for control signal at PHY-ES.
2) *SEK-based DSE Scheme*: A SEK-based DSE scheme is proposed, where the SEKs are generated by quantifying the randomness of the sensing data, without the need for any external key sources to encrypt the sensing data in the physical layer directly. The encryption process of the scheme is divided into initial SEK generation, SEK matrix creation, disarrangement of both SEKs and sensing data, etc.
3) *Novel SEK-based DSE Algorithm and its Experimental Platform*: We establish a novel SEK-based DSE algorithm and verify its feasibility by simulations. Meanwhile, we build an experimental platform to validate the proposed scheme and algorithm. The experimental results are consistent with their simulation counterparts. Compared with other schemes, the SEK-based DSE scheme is able to reduce the data life cycle (DLC) and average cost (AC) by around 42% and 35% on average, respectively.

The remainder of this paper is organized as follows. Section II proposes the PHY-ES architecture and the SEK-based DSE scheme. Section III details the process, algorithm, and simulation for the scheme. Section IV presents the experimental approach and system and discusses the testing results. Finally, Section V concludes this article.

II. Architecture and Scheme

In this section we provide a solution that combines suitable physical layer architectures and security functions without using external key source for IoT sensing data in the physical layer of IoT. The PHY-ES architecture suitable for the generic scenario of IoT and the SEK-based DSE scheme are proposed.

A. PHY-ES Architecture for IoT

The PHY-ES architecture with both endogenous encryption and decryption functions for IoT systems is shown in Fig.1. In addition to supporting the basic functions of the traditional Ethernet physical layer architecture, such as transmission medium connection, encoding/decoding, serial-to-parallel conversion, etc. [18, 19], the novel architecture proposed here also provides both the endogenous encryption and decryption functions for sensing data. Thus, the architecture consists of sensing sublayer (SS), physical function sublayer (PFS), and

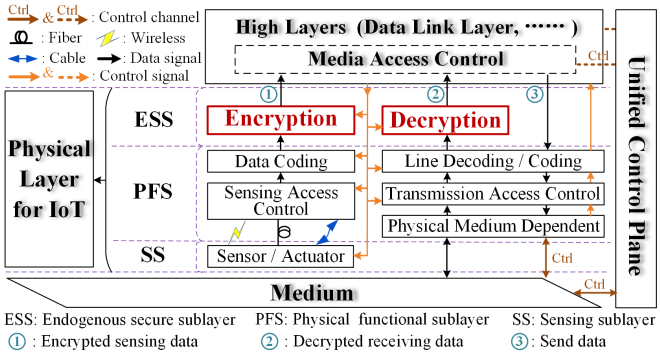


Fig. 1: PHY-ES architecture with both the endogenous encryption and decryption functions for IoT.

endogenous security sublayer (ESS). The control signals from the unified control plane are transmitted by an independent control channel, received by physical medium dependent, sent to higher layers, and then distributed to the corresponding functional modules at different functional sublayers. Thus, the control signals can directly manage the three sublayers at physical layer. For distinguishing between the control channels and control signals, the brown solid lines and dashed lines of Ctrl represent the actual and virtual control links, respectively, and the orange solid lines on the right and at the middle are the control signals, as shown in Fig.1.

The SS is composed of sensors and actuators for collecting sensing data and can be connected simultaneously with the PFS via optical fiber, cable, and wireless connections, or any one of them. The PFS provides connections between the SS and ESS, and between the medium and ESS, as well as provides access control, encoding/decoding, and other functions for sensing data. The ESS contains both endogenous encryption and decryption functions for generating SEKs without any external key source systems, encrypting and decrypting the sensing data directly at the physical layer.

There are many advantages of the PHY-ES architecture for the IoT. First, this architecture is highly compatible, providing both endogenous security functions and traditional physical layer functions. Then, the SEKs are generated directly from the sensing data accessed in the physical layer without any external key sources, so that the SEKs are not vulnerable to be interfered or intercepted by attackers, conducing to improve the security and stability and reduce the overhead for the physical layer. And both the encryption and decryption functions are transparent to the multi-source heterogeneous sensing data, and process the data with any length at one time, to enhance the flexibility of the physical layer. Finally, the SEK-based DSE scheme can encrypt huge amounts of multisource heterogeneous sensing data within the edge access nodes, adapt to the IoT networks with different size and changing environment, and has strong scalability.

B. SEK-based DSE Scheme

For achieving both the endogenous encryption and decryption functions of the PHY-ES architecture shown in Fig.1, a SEK-based DSE scheme implemented at the ESS is proposed in Fig.2. For ease of exposition, nodes n and m in Fig.2

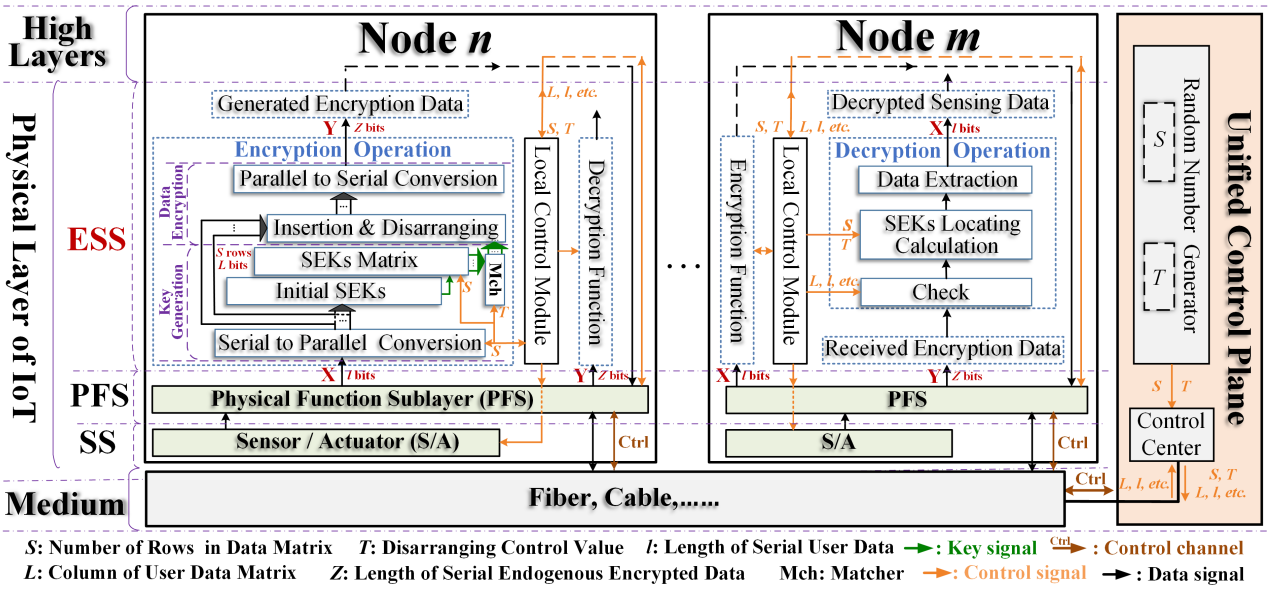


Fig. 2: SEK-based DSE scheme for the PHY-ES architecture of IoT.

represent the physical layer in Fig.1 (n, m=1, 2, …, $n\neq m$), and provide the encryption and decryption of the scheme in ESS in detail as follows, respectively, and the frameworks of PFS and SS are the same as those in Fig.1.

First of all, a unified control plane generates the random numbers S and T as the control parameters for the scheme of node n. The long serial sensing data X with a length of l bits from the SS are sliced and converted into a data matrix with S rows through the serial to parallel part, and each row in the data matrix has the same length L. By quantifying the randomness in the column space of the data matrix, the initial SEKs related to the values of L columns in the data matrix are generated in the initial SEKs part. Therefore, the SEKs matrix can be created with S rows and B columns ($B = \lfloor L/S \rfloor$).

Subsequently, according to control parameter T, the SEKs matrix needs to be inserted into the data matrix. In this way, the data matrix arrangement has been completely disarranged by inserting the SEKs matrix.

Subsequently, the endogenous encrypted sensing data Y with a length of Z bits (Z=l+L) are obtained by parallel to serial conversion. At this point, endogenous encryption of the original sensing data has been completed.

The series of parameters generated during the above encryption process (such as l, L, etc.) are directly fed back to the unified control plane and then sent to the check part at node m. Thus, encrypted sensing data Y is received and can be checked at this node. By finding the corresponding S and T, and calculating the SEK locations of Y, X can quickly and accurately decrypt from the checked Y.

III. Process, Algorithm and Verification

In order to implement the SEK-based DSE scheme for the PHY-ES architecture, this section details the process of the scheme, establishes the corresponding algorithm, and finally verifies the performance of the scheme by simulation.

A. Process of SEK-based DSE Scheme

The encryption process of the SEK-based DSE scheme is shown in Fig.3, where input port 1 inputs S and T, input port 2 inputs sensing data X, and output port outputs endogenous encrypted sensing data Y. After X is sliced and converted into a data matrix $\mathbf{X}$ with S rows and L columns in the serial to parallel part, the randomness of the column in $\mathbf{X}$ is quantified in the initial SEKs part [20]. In the matrix part, the quantification result of $\mathbf{X}$ is an SEK matrix $\mathbf{K}$ with S rows and B columns generated based on the initial SEKs. The i-th row of $\mathbf{K}$ is inserted into the corresponding row of $\mathbf{X}$, the $\mathbf{K}$ includes k_{i-1}~k_{i-B}, where i is the row order, $1 \le i \le S$. After matching $\mathbf{K}$ with T_i, in the insertion and disarranging part, $\mathbf{X}$ and $\mathbf{K}$ are disarranged according to T_i. When i=S, Y_S is obtained by combining and disarranging the sensing data x_{S1}~x_{SL} with SEKs k_{S-1}~k_{S-B} based on T_S. After the parallel to serial conversion, Y: y_1~y_Z is the output.

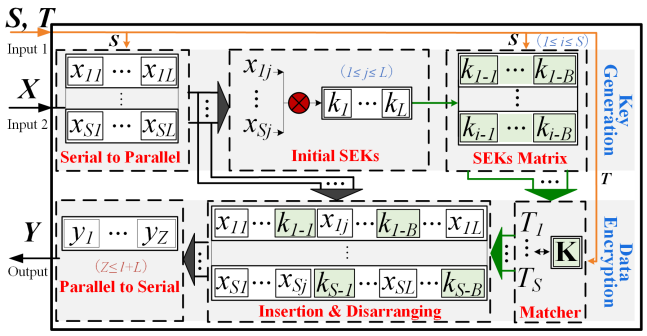


Fig. 3: Encryption process of SEK-based DSE scheme.

The decryption process of the SEK-based DSE scheme is shown in Fig.4. The input port 1 inputs the endogenous

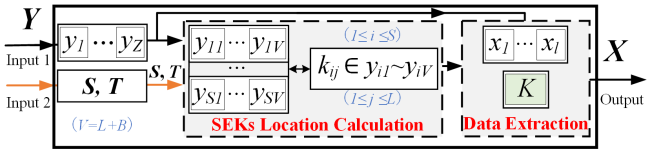


Fig. 4: Decryption process of SEK-based DSE scheme.

encrypted sensing data Y, the input port 2 inputs S and T. Theoutput port outputs the decrypted sensing data X. When Y: $y_1 \sim y_Z$ is received and checked successfully, in the SEK location calculation part, the location of SEK k_{ij} is calculated in a data matrix composed by $y_1 \sim y_Z$ based on S and $T_1 \sim T_S$. Then, in the data extraction part, the sensing data $x_1 \sim x_l$ are separated from Y, and X is the output, where $V=L+B$.

B. Algorithm of SEK-based DSE Scheme

According to the SEK-based DSE scheme, we give the corresponding algorithm as follows

$$\begin{aligned} \mathbf{Y} &= E(\mathbf{X}) \\ &= \prod_{v=1,2,3} E_v(\mathbf{X}) = E_1\{E_2[E_3(\mathbf{X})]\} \end{aligned} \tag{1}$$

where $\mathbf{X}$ with S rows and L columns is the input matrix, $\mathbf{Y}$ is the output matrix of, and E is the encryption algorithm.

According to the encryption process in Fig. 3, E can be divided into algorithms E_1, E_2, and E_3 for generating initial SEKs, creating SEKs matrix, and inserting SEKs into sensing data by disarranging, respectively. Each of the three algorithms is described in pseudocode as follow.

Algorithm $\mathbf{E}_1$: Input: $\mathbf{X}_1$=$\mathbf{X}$; Require: $\mathbf{Y}_1$

for j = 1:1:L do
  $\mathbf{E}_1(j)$ = 0;
  for i = 1:1:S do
    $\mathbf{E}_1(j)$ = *Calculate* [$\mathbf{E}_1(j)$, $\mathbf{X}_1(i,j)$];
  end for
  $\mathbf{Y}_1(j)$ = $\mathbf{E}_1(j)$;
end for
output [$\mathbf{Y}_1(1)$, …, $\mathbf{Y}_1(L)$]

where $\mathbf{X}_1$=$\mathbf{X}$ is the input matrix, $\mathbf{E}_1$ is the generation matrix of the initial serial SEKs, output matrix $\mathbf{Y}_1$ is the initial serial SEKs. The *Calculate* function quantifies the column randomness of $\mathbf{X}_1$. $\mathbf{X}_1(i, j)$ is the element of $\mathbf{X}_1$ in the i-th row and j-th column, $\mathbf{E}_1(j)$ is the j-th column of $\mathbf{E}_1$, $\mathbf{Y}_1(j)$ is the j-th element of $\mathbf{Y}_1$.

Algorithm $\mathbf{E}_2$: Input: $\mathbf{X}_2$=$\mathbf{Y}_1$; Require: $\mathbf{K}$ = $\mathbf{Y}_2$

initial $B = \lfloor L/S \rfloor$;
for i = 1:1:S do
  $\mathbf{Y}_2(i) = \mathbf{X}_2 \cdot \mathbf{E}_2(i) = \mathbf{Y}_1 \cdot (\mathbf{O}_1, \ldots, \mathbf{I}_i, \ldots, \mathbf{O}_S)'$;
end for
output $\mathbf{K} = \mathbf{Y}_2 = \begin{bmatrix} \mathbf{Y}_2(1) \\ \vdots \\ \mathbf{Y}_2(S) \end{bmatrix}$

where $\mathbf{X}_2$=$\mathbf{Y}_1$ is the input matrix, $\mathbf{Y}_2$ is the output matrix with S rows and B columns, $\mathbf{Y}_2(i)$ is the i-th row of $\mathbf{Y}_2$, $\mathbf{E}_2$ is the generation matrix of the SEKs matrix and consists of S small matrices with only one small matrix is the identity matrix $\mathbf{I}$ and the others are all zero matrix $\mathbf{O}$. $\mathbf{K}$ is the SEK matrix.

In X_3 is the input matrix consisting of the $\mathbf{X}$ and the $\mathbf{K}$, $\mathbf{Y}_3$ is the output matrix. The function $E_3\{\mathbf{X}_3, i, T_i\}$ represents that the i-th row of $\mathbf{K}$ is inserted into the i-th row of $\mathbf{X}$ and multiplied by 2^{Ti}, so as to disarrange the i-th row of $\mathbf{X}$ and $\mathbf{K}$.

Algorithm $\mathbf{E}_3$: Input: $\mathbf{X}_3$=$\mathbf{X}$ and $\mathbf{K}$; Require: $\mathbf{Y}$=$\mathbf{Y}_3$

initial $T = (T_1, \ldots, T_S)$;
for i = 1:1:S do
  $\mathbf{Y}_3(i) = E_3\ [\mathbf{X}_3, i, T_i]$;
end for
output $\mathbf{Y} = \mathbf{Y}_3 = \begin{bmatrix} \mathbf{Y}_3(1) \\ \vdots \\ \mathbf{Y}_3(S) \end{bmatrix}$

And the algorithm for decryption process is shown below.

$$D(\mathbf{Y}) = D[E(\mathbf{X})] = \mathbf{X} \tag{2}$$

where D is the decryption algorithm that is described as follows.

We define $\mathbf{Y}(i)$ as the i-th part of $\mathbf{Y}$, $\mathbf{X}(i)$ is the i-th row of $\mathbf{X}$, the $D\{\mathbf{Y}(i)\}$ is responsible for resetting $\mathbf{Y}(i)$ and extracting $\mathbf{X}(i)$ form it, composed by an $\mathbf{I}$ and an $\mathbf{O}$.

Algorithm D: Input: $\mathbf{Y}$; Require: $\mathbf{X}$

initial $V = L + B$;
for i = 1:1:S do
  $\mathbf{Y}(i)$ = [$Y_{1+V\cdot(i-1)}$, …, $Y_{V\cdot i}$];
  $\mathbf{X}(i)$ = D[$\mathbf{Y}(i)$] = [$\mathbf{Y}(i)\cdot 2^{-Ti}$] · ($\mathbf{I}$ $\mathbf{O}$)$_i$';
end for
output $\mathbf{X} = \begin{bmatrix} \mathbf{X}(1) \\ \vdots \\ \mathbf{X}(S) \end{bmatrix}$

C. Performance Evaluation Method

To evaluate the performance of the SEK-based DSE scheme, we determine a special parameter as DLC, which represents the duration time T_{DLC} of sensing data confidentiality at the physical layer of IoT. T_{DLC} is defined as following

$$T_{DLC} = T_e + T_d + T_t + T_a \tag{3}$$

where T_e and T_d are the processing time spent in the encryption module and decryption modules, respectively. T_t is the transmitting time in medium. T_a is the additional time, such as the modulation, demodulation, encoding, queuing, and so on.

$$\begin{cases} t_e = T_e/l \\ t_d = T_d/Z \\ n_e = Z/l = 1 + L/l \end{cases} \tag{4}$$

Meanwhile, we determine another special parameter as AC, including t_e, t_d, and n_e, where t_e and t_d are the average time required for encrypting and decrypting each bit of sensing data, respectively, n_e is the average bits required for encrypting each bit of sensing data. It is obvious that the smaller the DLC

is and the lower the AC is, the better the performance of the SEK-based DSE scheme for the PHY-ES architecture is.

The time of the illegal node forcibly deciphers encrypted sensing data is defined as T_i, and represented by the combination of T_e, T_d, and coefficients ϕ and γ.

$$T_i = (\frac{L^*}{2} - 1)^2 \cdot S^* \cdot T^* \times (\phi \cdot T_e + \gamma \cdot T_d) \quad (5)$$

where L^* is length of the intercepted encrypted sensing data, S^* and T^* are the values of S and T guessed by external illegal nodes, respectively. Then the deciphering probability η as follows

$$\eta = T_d/T_i = \frac{1}{(\frac{L^*}{2} - 1)^2 \cdot S^* \cdot T^* \times (\phi \cdot \frac{T_e}{T_d} + \gamma)} \quad (6)$$

where η is the ratio of T_i to T_d for the same encrypted sensing data. Therefore, the greater the difference between T_e and T_d is, and the longer L is, the larger the value range of S and T is, then the smaller the η is and the higher the security of the encrypted sensing data is.

All in all, in addition to DLC, AC, and η mentioned above, the SEK-based DSE scheme can also be evaluated from other different perspectives, such as energy consumption, algorithm complexity, and so on. And the IoT physical layer has to face the similar security threats as those existing in the current Internet, including eavesdropping, interference, sabotage, etc. The SEK-based DSE scheme has strong defensive capabilities when dealing with eavesdropping threats, but it is still necessary to conduct research on corresponding defense mechanisms against other attacks to ensure the PHY-ES of IoT.

D. Simulation of SEK-based DSE Scheme

Based on the process, algorithm, and method of SEK-based DSE scheme built above, we simulate the scheme in MATLAB, and analyze and verify the changes of the DLC and AC with different sensing data lengths. And the system time of MATLAB is unified as the unit time (u.t).

We simulate the DLC for the scheme draw the curves of T_{e-s}, T_{d-s}, and T_{DLC-s} as L increases from 1×10^3 bits to 10×10^3 bits with S=10, S=50, and S=100, as shown in Fig.5, so as to explore the suitable length of slicing. In Fig.5, T_{e-s} and T_{d-s} are defined as the processing times of encryption and decryption in simulations, respectively, and T_{DLC-s} is the duration time of the sensing data encrypted by the SEKs at the physical layer of IoT in simulations.

In Fig.5 (a), by comparing the curves with the same color, T_{e-s} is larger than T_{d-s}, e.g., blue curves, when S=100 and L=10×10^3 bits, T_{e-s}=66.3 u.t > T_{d-s}=25.5 u.t. When L is fixed, regardless of the value of S, the gap between T_{e-s} and T_{d-s} becomes larger with the increase of S. For example, when L=10×10^3 bits, the value of $\Delta(T_{e-s}\text{-}T_{d-s})$ increases by approximately 89.7 times as S increases from 10 to 100. Since the time complexity of the encryption algorithm is nonlinear, while the decryption algorithm is linear, T_{e-s} is significantly larger than T_{d-s}, and $\Delta(T_{e-s}\text{-}T_{d-s})$ widens, as the total amount of sensing data increases.

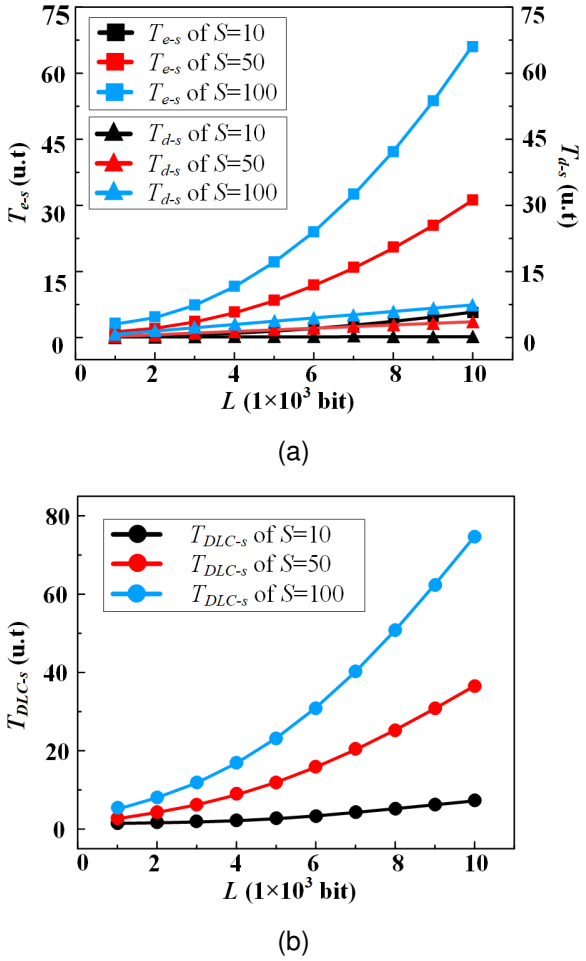


Fig. 5: Simulation results of how (a) T_{e-s}, T_{d-s}, and (b) T_{DLC-s} vary with L.

In Fig.5 (b), assuming T_t+T_a =1 u.t in simulations, when S is constant, as L increases, T_{DLC-s} increases, and the larger S is, the faster T_{DLC-s} increases. Although, it is noted that the curve of T_{DLC-s} is similar to that of T_{e-s} with the same S in Fig. 5 (a), they are not completely consistent.

Then, we carry out a simulation of the AC for the scheme, and draw the curves about t_{e-s}, t_{d-s}, and n_{e-s} as L increases from 1×10^3 bits to 10×10^3 bits under the conditions of S=10, S=50, and S=100, as shown in Fig.6, where t_{e-s} and t_{d-s} are the average times required for encrypting and decrypting each bit of sensing data in the simulations, respectively, and n_{e-s} is the average number of bits required for encrypting each bit of sensing data in the simulations.

In Fig.6 (a), when S is fixed, the trends of curves t_{e-s} and t_{d-s} are opposite to those of T_{e-s} and T_{d-s}, respectively. With an increase in L, t_{e-s} and t_{d-s} decrease, and both reach the minimum value at approximately L=8×10^3 bits. When S=100, the minimum values of t_{e-s} and t_{d-s} are 0.678×10^{-4} u.t and 0.235×10^{-4} u.t, respectively, whereas when S=10, the minimum values of t_{e-s} and t_{d-s} are 0.536×10^{-4} u.t, and 0.109×10^{-4} u.t, respectively.

In Fig.6 (b), when S is fixed, with the increase of L, n_{e-s} decreases during L=1×10^3~4×10^3 bits, and then becomes stable during L=8×10^3~10×10^3 bits. Obviously, n_{e-s} starts approaching the minimum value around L=8×10^3 bits under

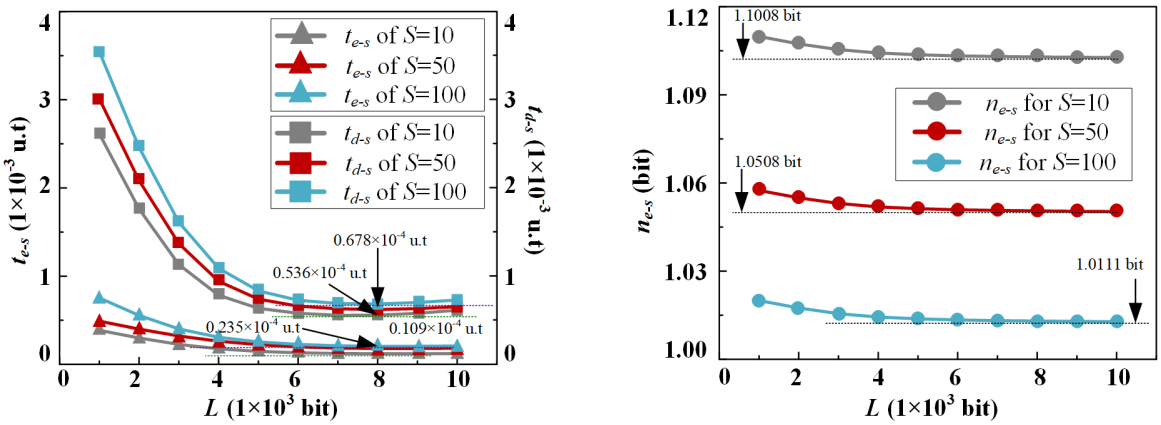


Fig. 6: Simulation results of (a) t_{e-s}, t_{d-s}, and (b) n_{e-s} vary with L.

all conditions, and the minimum values of n_{e-s} for S=10 and S=100 are 1.1008 and 1.0111 bits, respectively. As can be observed from the figure, the less the slicing length of the sensing data, the smaller the DLC is and the better the sensing data confidentiality, but the higher the AC.

IV. Experiments and Discussions

According to the above process, algorithm, and simulation of the scheme proposed here, for further verification, we need to explore a simplified experimental approach, build an experimental system at the lab, and discuss the experimental results. Meanwhile, we compare the experimental results with similar reported schemes.

A. Experimental Scheme

We design an experimental platform for the SEK-based DSE scheme suited for the PHY-ES architecture as shown in Fig.7, in which two physical layer nodes with a small form pluggable (SFP) interface each are connected by using a section of optical fiber. Node 1 encrypts the sensing data sent from the sensing database, transmits the encrypted sensing data to node 2 and the server computer through optical fiber and a universal serial bus (USB) interface respectively. After decrypting the encrypted sensing data at node 2, it is sent to the server computer through a USB interface in the node. To simplify the experimental system, the computer has both control signal transmission and encrypted/decrypted sensing data reception functions, and is directly connected to two nodes through USB interfaces, by using the cable. Thus, the control parameters S and T are sent to the two nodes directly. At the same time, the sensing data at the bottom left in node 1 can be produced by the random number generator. During the testing process, we mainly focus on verifying the SEKs generation and both encryption and decryption functions.

According to the approach above, we set up an experimental system with two physical layer nodes for SEK-based DSE scheme, implemented by using a FBGA (Xilinx KC705) board, as shown in Fig.8 in the lab. Two FPGA boards are connected with each other through a single mode fiber G.652D with 10 kilometers and SFP optical transceivers. The server computer and monitor are directly connected to the two boards through USB interfaces and cable, so that the encrypted sensing data Y and decrypted sensing data X can be displayed on the monitor.

Figs.9 (a) and (b) illustrate the flow chart for data processing of encryption and decryption of the SEK-based DSE scheme, on which the software is developed by the Vivado and inserted in two nodes, respectively. To observe the processing time of encryption and decryption at the debug window of an integrated logic analyzer, respectively, a counter is both set

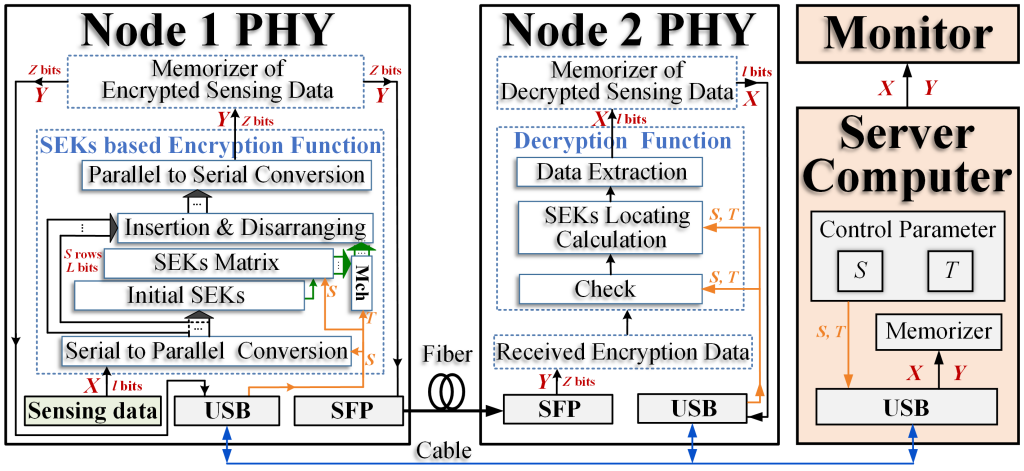


Fig. 7: Experimental platform for the SEK-based DSE scheme suited for the proposed PHY-ES architecture.

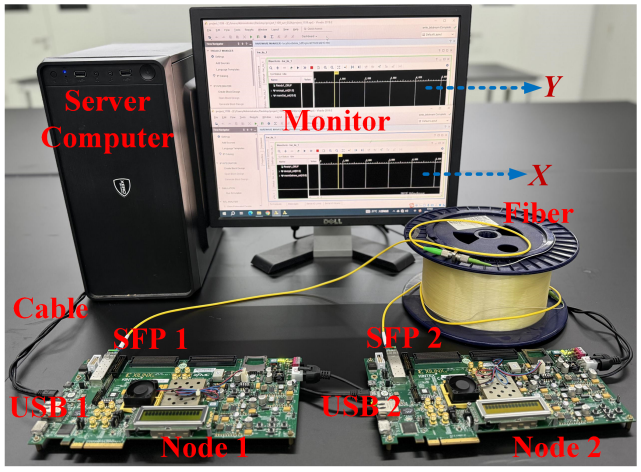


Fig. 8: Experimental system of the SEK-based DSE scheme built in our lab.

and turned on at the start of encryption and decryption, and is both stopped and outputted the counter results at the end.

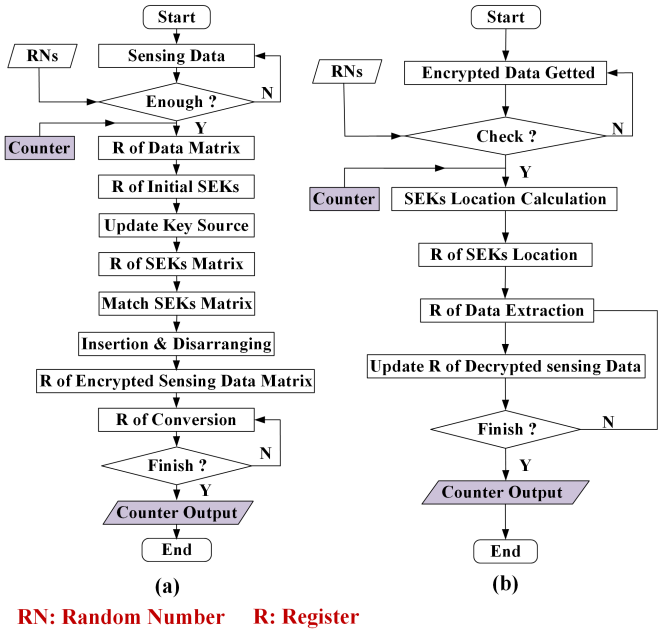


Fig. 9: Flow chart for data processing about (a) encryption and (b) decryption of SEK-based DSE scheme on FPGA.

The experiment results of nodes 1 and 2 are shown in Figs.10 (a) and (b), where Ready1_OBUF=1 indicates that the encryption or decryption is in progress, encrypt_cnt and decrypt_cnt indicate T_e and T_d, respectively. Due to the total number limitation of the observable bits in waveform of debug window, the encrypted sensing data and the decrypted sensing data cannot be observed, we estimate the ne roughly by counting the number of "1" codes in data, based on the law of large numbers. The memGet_cnt and memGetnew_cnt are used to indicate the number of "1" codes in encrypted sensing data and the decrypted sensing data, respectively.

B. Results and Discussions

During the testing, we repeat two hundred times and average the testing data to draw the experimental results for each one.

Figs.11 (a) and (b) depict how T_{e-e} and T_{d-e} vary with L under different values of S, and compare the obervations with the simulated ones for T_{e-s} and T_{d-s}, respectively. T_{e-e} and T_{d-e} are defined as the processing time for encryption and decryption on nodes 1 and 2, respectively. If L and S are constant, T_{e-e} is always greater than T_{d-e}. And only S is constant, both T_{e-e} and T_{d-e} increase with L, but the rate of increase of T_{e-e} is obviously faster than that of T_{d-e}. When only L is fixed, the larger S is, the larger T_{e-e} and T_{d-e} are.

The above experimental results are almost consistent with the simulation results shown by the solid line with light blue, light red and light black in Figs.11 (a) and (b). However, there are some differences between T_{e-e} and T_{e-s}, as well as T_{d-e} and T_{d-s}, which are caused by the delay deviation stemming from FPGA logic circuit instability, power instability, register reading, and so on.

Fig.12 shows T_{DCL-e} varies with L under the conditions of S=10, S=50, and S=100, and compares T_{DCL-e} with the simulation values, where T_{DCL-e} is the duration of the sensing data encrypted by SEK at the physical layer of IoT in the experiments. Meanwhile, we assume that the transmit time T_t and additional time T_a are calculated according to the length of fiber, the number of bits transmitted, as well as the transmission rate of SFP during testing.

As can be observed from Fig.12, the value of T_{DCL-e} is similar to T_{DCL-s}, but the values of T_{DCL-e} values are always slightly larger than the simulated ones with values of S and L. The larger S and L are, the larger the difference between T_{DCL-e} and T_{DCL-s} is. This is because the transmission time T_a for encrypted sensing data is constant in simulation, but it is a variable in experiment and varies with total amount of transmitted data.

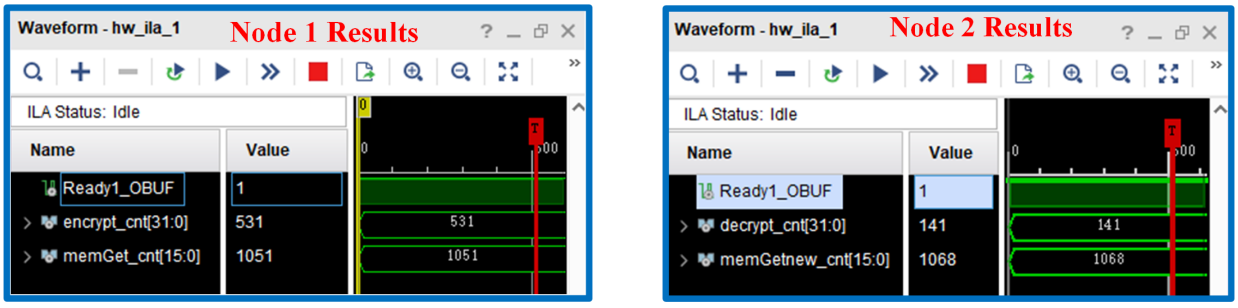
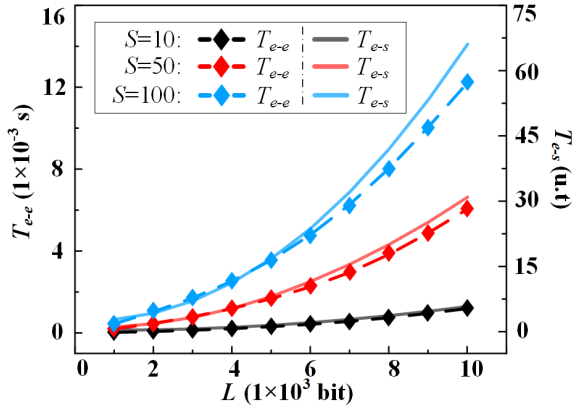
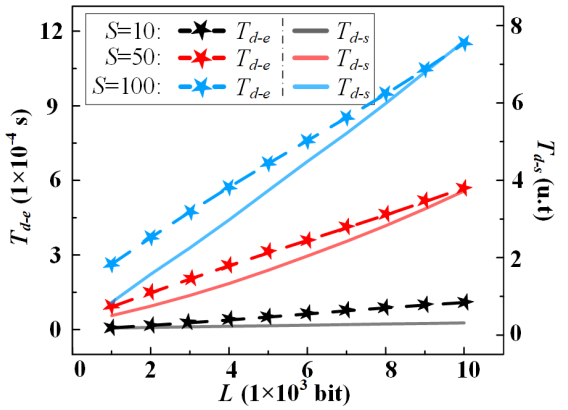


Fig. 10: Experiment results of (a) node 1 and (b) node 2.

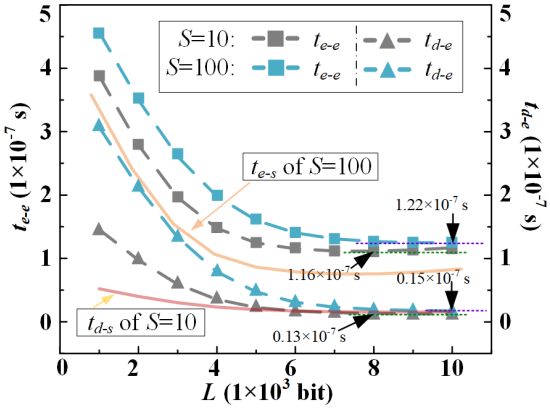


(a)

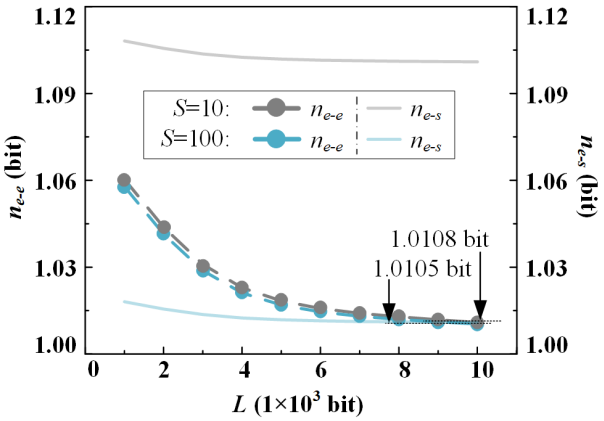


(b)

Fig. 11: Experimental results of (a) T_{e-e} and (b) T_{d-e}, change with L, and compared with the simulation ones for T_{e-s} and T_{d-s}, respectively.



(a)



(b)

Fig. 13: Experimental results of (a) t_{e-e} and (b) n_{e-e}, change with L, and compared with the simulation ones for t_{e-s} and n_{e-s}, respectively.

Fig.13 (a) depicts t_{e-e} and t_{d-e} vary with L, and the comparison with the simulation ones for t_{e-s} and t_{d-s}, where t_{e-e} and t_{d-e} are the average time required for encrypting and decrypting each bit of sensing data in experiments, respectively. When L is fixed, the larger S is, the larger t_{e-e} and t_{d-e} are. When S is fixed, as L increases, t_{e-e} and t_{d-e} gradually tend to the minimum value, which are opposite to the change trend of T_{e-e} and T_{d-e}, respectively. When S=100, t_{e-e} and t_{d-e} approach the minimum values of 1.22×10^{-7} s and 0.15×10^{-7} s, around L=10×10^3 bits, respectively. However, when S=10, t_{e-e} and t_{d-e} approach the minimum values of 1.16×10^{-7} s and 0.13×10^{-7} s, around L=8×10^3 bits, respectively. And the experimental results have some differences with the simulations shown by the orange and red solid lines, which are caused by the delay deviation of the FPGA board, the transmission hysteresis of the control signal during test, etc.

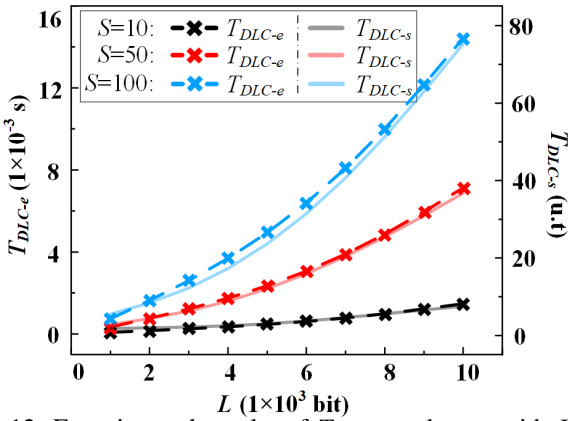


Fig. 12: Experimental results of T_{DCL-e} change with L, and compared with the simulation ones for T_{DCL-s}.

Fig.13 (b) plots n_{e-e} based on the assumption that the codes for bits "1" and "0" are the same in one sensing data bit, and compared with the n_{e-s}, where n_{e-e} is the average number of bits required for encrypting each bit of the sensing data in the experiments. As can be seen from the figure, n_{e-e} decreases as L increases, and around L=8×10^3 bits, it tends to approach the minimum value under all sensing data lengths, which is almost same as the simulation results in Fig.6 (b). However, there are some differences between the experimental and simulated results shown by the solid line with lighter color for the case of S=10 with all values of L and the case of S=100 with L=1×10^3 bits~6×10^3 bits. Since the above assumption is based on the law of large numbers, and the longer the length of the sensing data is, the closer the experimental results to their simulated counterparts are.

C. Performance Comparisons

Among many physical layer encryption schemes for IoT, deep learning-based schemes have better performance than other ones. Therefore, this section compares the performance of the SEK-based DSE scheme with the key generation neural network (KGNet) presented in [16] and the bidirectional convergence feature learning (BCFL) network presented in [17]. Firstly, the biggest difference between the proposed scheme in this paper and the latter two is that the former uses SEKs, while the latter two require external key sources.

Next, we compare the performance of three schemes under different total amounts of sensing data l, where the execution time and key generation amount in per unit time of both [16] and [17] are similar to the T_{e-e} and n_{e-e} of the experimental results of our scheme.

Fig.14 compares the T_{e-e} results of our scheme with those of the KGNet and BCFL when l=1×10^3, 50×10^3, and 100×10^3 bits, respectively. It is obvious that T_{e-e} of our scheme is better than those of the KGNet and BCFL, and the larger the l, the greater the T_{e-e} difference of the three schemes. In particularly, when l=100×10^3 bits (purple column), the T_{e-e} of our scheme reduces by 75.22% and 18.65%, compared with the KGNet and BCFL, respectively.

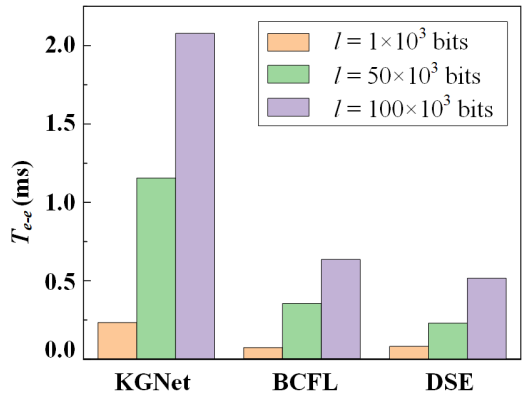


Fig. 14: T_{e-e} comparison of our scheme with KGNet and BCFL.

The reason why DSE performs better in Fig.14 is that the KGNet and BCFL are both traditional encryption schemes with classical external key source, while the DSE scheme can generate SKEs and encrypt sensing data inside the IoT physical layer system. It is future means that the novel idea of endogenous key source proposed in this paper can effectively improve the encryption performance of massive sensing data at the physical layer of IoT.

Fig.15 compares n_{e-e} of our scheme with those of the KGNet and BCFL when l=1×10^3, 50×10^3, and 100×10^3 bits. When l is small, the n_{e-e} for our scheme is approximately equal to that for KGNet, and both are greater than that for BCFL. When l is larger, e.g. l=100×10^3 bits (purple column), compared to KGNet and BCFL, our scheme performs better and reduces by 24.13% and 47.2% for n_{e-e}, respectively. As l increases, the n_{e-e} values of the three schemes tend to their respective minimum values, respectively. The reason of DSE performs better than KGNet and BCFL is same as above.

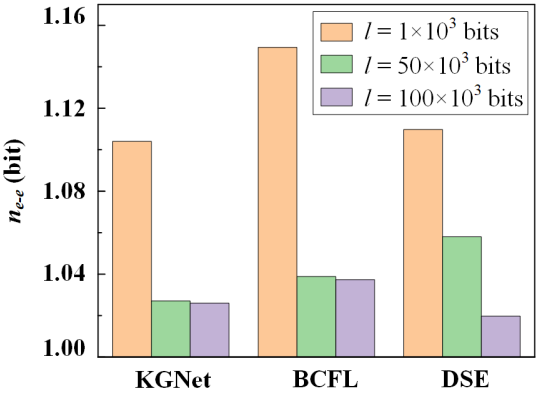


Fig. 15: n_{e-e} comparison of our scheme with KGNet and BCFL.

To summarize, we conclude that the SEK-based DSE scheme for the PHY-ES architecture of IoT has high security and low overhead without needing any external key source. Compared with the KGNet, T_{e-e} and n_{e-e} of our scheme are reduced by 75.22% and 24.13%, respectively, while the reeducations are 18.65% and 47.2% compared with the BCFL, respectively.

V. Conclusion

In this paper a novel PHY-ES architecture and an SEK-based DSE scheme suited for IoT were proposed. The motivation of this architecture was to provide both endogenous encryption and decryption functions for massive amounts of heterogeneous sensing data in the physical layer, especially for unique scenes of IoT, where the sensing data traffic in the uplink is far larger than the one of the downlinks. The scheme can generate SEKs by quantifying the randomness of sensing data without any external key source, encrypt and decrypt the sensing data directly in the physical layer. After the detailed process of the scheme is given, a corresponding algorithm for the scheme was established and its simulation results were analyzed. A simplified experiment platform was constructed, on which the performance of the SEK-based DSE scheme for PHY-ES architecture was demonstrated to be viable and effective for protecting the sensing data, and can reduce the DLC and AC on average by about 42% and 35%, compared with other schemes, respectively. All in all, the PHY-ES architecture and the SEK-based DSE scheme proposed in this paper provide a unique and advantageous approach for accessing to massive heterogeneous sensing data securely in IoT.

Currently, due to the diverse functions and types of sensors and actuators, the actually deployed IoT will face the challenges, such as multi-source heterogeneous sensing data access, unstable uplink channels, eavesdropping attacks, etc. Although the SEK-based DSE scheme can adapt to the relatively complex conditions of IoT, with the rapid development of IoT technologies in application, there are still some research works to be carried out in security analysis, practical deployment, scalability, and energy consumption of SEK-based DSE scheme. Firstly, by combining the artificial intelligence algorithms to strengthen the preprocessing of sensing data, the security of SEK-based DSE scheme can be improved. Secondly,

the efficient sensing data access and aggregation schemes should be considered with the SEK-based DSE scheme to enhance its performance in complex network environments. Finally, we should expand the evaluation parameters, such as energy consumption, algorithm complexity, etc., and analyze the SEK-based DSE scheme from more perspectives.

REFERENCES

[1] A. Hazra *et al.*, "Fog computing for next-generation Internet of Things: Fundamental, state-of-the-art and research challenges," *Computer Sci. Rev.*, vol. 48, May 2023.

[2] J. Lin *et al.*, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," *IEEE Internet Things*, vol. 4, no. 5, pp. 1125-1142, Oct. 2017.

[3] S. Baker *et al.*, "Artificial Intelligence of Things for Smarter Healthcare: A Survey of Advancements, Challenges, and Opportunities," *IEEE Commun. Surv. Tut.*, vol. 25, no. 2, pp. 1261-1293, Jun. 2023.

[4] J. Ahmad *et al.*, "Machine learning and blockchain technologies for cybersecurity in connected vehicles," *Wires. Data Min. Knowl.*, vol. 14, no. 1, Sep. 2023.

[5] Y. F. Han *et al.*, " Reputation-aware rate maximization for cross-media cooperative transmission in smart ocean IoT," *IEEE Internet Things*, vol. 10, no. 20, pp. 19062-19074, Nov. 2023.

[6] Overview of the Internet of Things, ITU-T Y.4000 Recommendation, 2012.

[7] Functional framework and capabilities of the Internet of Things, ITU-T Y.4401 Recommendation, 2015.

[8] N. Abbas *et al.*, "Mobile Edge Computing: A Survey," *IEEE Internet Things*, vol. 5, no. 1, pp. 450-465, Feb. 2018.

[9] Sensor control networks and related applications in a next generation network environment, ITU-T Y.4250 Recommendation, 2013.

[10] IEEE Standard for broadband over power line networks: medium access control and physical layer specifications, IEEE Std 1901TM-2020 (Revision of IEEE Std 1901-2010), 2021.

[11] Y. D. Fu *et al.*, "High-speed optical secure communication with an external noise source and an internal time-delayed feedback loop," *Photonics Res.*, vol. 7, no. 11, pp. 1306-1313. Nov. 2019.

[12] J. B. Perazzone *et al.*, "Artificial Noise-Aided MIMO Physical Layer Authentication with Imperfect CSI," *IEEE T. Inf. Foren. Sec.*, vol. 16, pp. 2173-2185, Jan. 2021.

[13] X. F. Tang *et al.*, "A Physical Layer Security-Enhanced Scheme in CO-OFDM System Based on CIJS Encryption and 3D-LSCM Chaos," *J. Lightwave Technol.*, vol. 40, no. 12, pp. 3567-3575, Jun. 2022.

[14] N. Jiang *et al.*, "Physical secure optical communication based on private chaotic spectral phase encryption/decryption," *Opt. Lett.*, vol. 44, no. 7, pp. 1536-1539, Apr. 2019.

[15] Y. K. Chen *et al.*, "Security Analysis of QAM Quantum-Noise Randomized Cipher System," *IEEE Photonics J.*, vol. 12, no. 4, pp. 1-14, Aug. 2020.

[16] X. W. Zhang *et al.*, " Deep-Learning-Based Physical-Layer Secret Key Generation for FDD Systems," *IEEE Internet Things*, vol. 9, no. 8, pp. 6081-6094, Apr. 2022.

[17] Y. R. Chen *et al.*, "Physical-Layer Secret Key Generation Based on Bidirectional Convergence Feature Learning Convolutional Network," *IEEE Internet Things*, vol. 10, no. 16, pp. 14864-14855, Aug. 2023.

[18] IEEE Standard for Ethernet, IEEE Std 802.3-2022 (Revision of IEEE Std 802.3-2018), 2022.

[19] IEEE/ISO/IEC Telecommunications and exchange between information technology systems – Requirements for local and metropolitan area networks – Part 3: Standard for Ethernet AMENDMENT 4: Physical layers and management parameters for 50 Gb/s,200 Gb/s, and 400 Gb/s operation over single-mode fiber, IEEE/ISO/IEC 8802-3:2021/Amd 4-2021, 2021.

[20] X. Ye *et al.*, "A Key Generation Scheme from Sensing Data for IoT Security," in *Proc. IEEE Conf. Commun. Net. Secy. (CNS)*, Orlando, USA, Oct. 2023, pp. 1-2.

Xiaokai Ye received the B.S. degree from Hainan University, Haikou, China, in July 2017. He is currently working toward the Ph.D. degree in electronic engineering with Southeast University, Nanjing, China. His research focuses on the physical layer security of IoT.

Tao Lv received the B.S. degree and the Ph.D degree in electronic engineering in 2016 and 2024 from Southeast University, Nanjing, China, respectively. His research focuses on optical sensing and long-haul optical communication.

Kun Huang received a PhD in Electronic Engineering from Southeast University in Nanjing, China in June 2024. He is working at Nari Group in Nanjing, China. His research focuses on sensor network access technology.

Jinhui Li received Ph.D. degrees in electronic engineering from the Southeast University, Nanjing, China, in 2001. After working for over 20 years in Fortune Global 500 companies, she joined Nanjing Xiguang Research Institute. Her research areas include signal processing, communication, the IoT.

Xuekang Shan received the PhD degree in optical fiber communications from University of Essex, UK, in 1995. He held senior technical positions in Fortune Global 500 companies for over 20 years. He has been a technical consultant of Nanjing Xiguang Research Institute since 2017. His research interests include optical fiber communications.

Wei Xiang (Senior Member, IEEE) received the B.Eng. and M.Eng. degrees in electronic engineer ing from the University of Electronic Science and Technology of China, Chengdu, China, in 1997 and 2000, respectively, and the Ph.D. degree in telecom munications engineering from the University of South Australia, Adelaide, SA, Australia, in 2004. He is currently the Cisco Research Chair of AI and IoT and the Director of the Cisco-La Trobe Centre for AI and IoT, La Trobe University, Melbourne, VIC, Australia.

Xiaohan Sun is currently a Professor with the Scholl of Electronics Science Engineering and the Director of the National Research Center for Optical Sensing/Communications Integrated Networking, Southeast University, Nanjing, China. Her research interests include optical communications and sensing, the IoT.

Responding letter to the Reviewer's comments for IoT-41406-2024

Manuscript ID: IoT-41406-2024

Title: A Physical Layer Endogenous Security Architecture with Dynamic Slicing Encryption for IoT

At the beginning of the new year, we are delighted to receive the email, and would like to express our sincere thanks to the Associate Editor and the Reviewers for the hard work and recognition of the manuscript, as well as their careful assessments and constructive comments, particularly the time being spent. The details are explained below. Revised parts are marked in red color in the revision.

Reply to Associate Editor

Comments: It is suggested that the authors further improve these aspects in subsequent research to enhance the practicality and universality of the scheme.

Reply: We would like to express our sincere thanks to you for the time and effort you spent, as well as understanding and recognition of this manuscript.

In the subsequent research, we will further improve our work in terms of security analysis, real-word development, scalability and flexibility, and energy consumption, etc., based on the reviewers' comments and suggestions, so as to enhance the practicality and universality of the SEK based DSE scheme.

In addition, we would like to thank you again and the IoT editorial team for your hard work and wisdom on our manuscript, your efforts and meticulousness have played a very important role in improving the quality of our manuscript.

Reply to Reviewer 1

Q1: Security Analysis: Although the paper mentions the security of SEK schemes, it is recommended that the authors further analyze the security threats and defense mechanisms that SEK schemes may face.

A1: Thanks, your thorough assessments and constructive suggestions about security analysis have been of utmost significance in enhancing the quality of this manuscript.

In IoT, the security threats faced by the physical layer are highly similar to those of the current Internet, covering eavesdropping, interference, and sabotage. However, the SEKs generated by quantifying the randomness of the aggregated massive amounts of sensing data, and the unified control plane of IoT will distribute and continuously update the control parameters (S and T) to its subscribed users, it demonstrates that the SEK schemes have strong defensive capabilities when dealing with

eavesdropping threats, and are extremely difficult to correctly decipher the encrypted sensing data even if it is intercepted by eavesdropping. Currently, our research group is studying in-depth research on defense mechanisms against other attacks to ensure the endogenous security of physical layer in IoT.

At the end of Part C in Section Ⅲ of the revised version, the security analysis has been added as following: *The physical layer of IoT has to face the similar security threats as those existing in the current Internet, including eavesdropping, interference, sabotage, etc. The SEK-based DSE scheme has strong defensive capabilities when dealing with eavesdropping threats, but it is still necessary to conduct research on corresponding defense mechanisms against other attacks to ensure the PHY-ES of IoT.*

Q2: Real-world deployment considerations: The proposed solution has been validated in a lab environment, but the authors are advised to discuss the challenges that the solution may encounter in real-world deployment, such as how it behaves under different network conditions and attack scenarios.

A2: Thanks very much for your careful comments and valuable suggestions on real-world deployment considerations.

At present, the real-world deployment of IoT basically adopts the conventional Internet architecture, and the sensing data are accessed at the edge of networks. Due to the diverse functions and types of sensors and actuators, they will face challenges such as multi-source heterogeneous sensing data access, unstable uplink channels, eavesdropping attacks, etc. However, since the SEK schemes are transparent to sensing data and have strong defensive capabilities when dealing with eavesdropping threats, in the actually deployed IoT, the SEK schemes can adapt to the relatively complex conditions and scenarios for accessing sensing data in IoT.

This discussion has been added to the second paragraph in Section Ⅴ (Conclusion) of the revised version: *Currently, due to the diverse functions and types of sensors and actuators, the actually deployed IoT will face the challenges, such as multi-source heterogeneous sensing data access, unstable uplink channels, eavesdropping attacks, etc. Although the SEK-based DSE scheme can adapt to the relatively complex conditions of IoT, with the rapid development of IoT technologies in application, there are still some research works to be carried out.*

Q3: Scalability and Flexibility: It is recommended that the authors explore the scalability and flexibility of the scheme in IoT networks of different sizes, and how to adapt to the changing network environment.

A3: We are sincerely grateful for your pertinent and insightful suggestion regarding the exploration of scalability and flexibility in IoT. It is highly thought-provoking.

The size of IoT networks depends on the number of the nodes at the physical layer. The larger the number of nodes, the greater the network scale. The SEK schemes are deployed in the edge access nodes for encrypting the sensing data, so as to ensure its security during uplink transmission. Therefore,

the scheme can be flexibly adapted to the IoT networks with different size and changing environment.

As one of the advantages of the SEK schemes, which has been added at the last paragraph of Part A in Section Ⅱ of the revised version: *The SEK-based DSE can encrypt huge amounts of multisource heterogeneous sensing data within the edge access nodes, adapt to the IoT networks with different size and changing environment, and has strong scalability.*

Q4: Energy consumption considerations: Energy consumption is an important consideration for IoT devices. It is recommended that the authors evaluate the energy consumption of the proposed scheme on actual IoT devices and compare it with existing scheme.

A4: We truly appreciate your suggestions on evaluating the energy consumption of our SEK schemes in IoT. And we'll act on them in the following research.

Based on the conventional processing of sensing data in the IoT physical layer, such as serial-to-parallel conversion, line encoding/decoding, etc., the SEK schemes achieve encryption by adding the key generation and data encryption functions. The schemes only add an encryption algorithm to the original hardware and computing resources of the edge access nodes for sensing data, without more additional energy consumption.

Since this paper mainly focuses on proposing and analyzing the security performance and cost of the SEK schemes, it fails to discuss and analyze the energy consumption issues of actual IoT devices and components in more detail, which is undoubtedly one of the main future research directions of our group. Nevertheless, the characterization of energy consumption has been added at Part C in Section Ⅲ of the revised version: *All in all, in addition to DLC, AC, and η mentioned above, the SEK-based DSE scheme can also be evaluated from other different perspectives, such as energy consumption, algorithm complexity, and so on.*

In summary, we would like to express our heartfelt gratitude to Reviewer 1 for your comprehensive and insightful comments and suggestions. The four advices above have pointed out the direction for our group to carry out the further research work on the SEK schemes. Therefore, at the second paragraph in Section Ⅴ (Conclusion) of the revised version, the above comments and suggestions are summarized again, as following:

With the rapid development of IoT technologies in application, there are still some research works to be carried out in security analysis, practical deployment, scalability, and energy consumption of SEK-based DSE scheme. Firstly, by combining the artificial intelligence algorithms to strengthen the preprocessing of sensing data, the security of SEK-based DSE scheme can be improved. Secondly, the efficient sensing data access and aggregation schemes should be considered with the SEK-based DSE scheme to enhance its performance in complex network environments. Finally, we should expand the evaluation parameters, such as energy consumption, algorithm complexity, etc., and analyze the SEK-based DSE scheme from more perspectives.

Reply to Reviewer 2

Comments: The PHY-ES architecture and SEK-based DSE scheme proposed in this paper have significant research value and application prospects in the field of IoT physical layer security. By generating endogenous keys and dynamic slicing encryption, they effectively address the secure transmission issues of massive heterogeneous sensing data, and have obvious performance advantages.

Reply: Thanks for your insightful and detailed comments of the PHY-ES architecture and SEK-based DSE scheme for IoT presented in our manuscript.

And your recognition and feedback not only validate our efforts but also spurs us on to deeper research and innovation in IoT physical layer security. We're committed to taking your comments and suggestions as our directions for continuous innovation and advancement in this crucial field.

Q1: There is room for improvement in aspects such as key security analysis, algorithm complexity assessment, and application scenario expansion. It is suggested that the authors further improve these aspects in subsequent research to enhance the practicality and universality of the scheme.

A1: Thank you very much for your constructive feedback. We fully acknowledge the areas you pointed out, including key security analysis, algorithm complexity assessment, and application scenario expansion.

In our upcoming research, we will center our efforts on SEK based DSE in following aspects, which have been added at the end of Section **V** in the revised version, as following:

Currently, due to the diverse functions and types of sensors and actuators, the actually deployed IoT will face the challenges, such as multi-source heterogeneous sensing data access, unstable uplink channels, eavesdropping attacks, etc. Although the SEK-based DSE scheme can adapt to the relatively complex conditions of IoT, with the rapid development of IoT technologies in application, there are still some research works to be carried out in security analysis, practical deployment, scalability, and energy consumption of SEK-based DSE scheme. Firstly, by combining the artificial intelligence algorithms to strengthen the preprocessing of sensing data, the security of SEK-based DSE scheme can be improved. Secondly, the efficient sensing data access and aggregation schemes should be considered with the SEK-based DSE scheme to enhance its performance in complex network environments. Finally, we should expand the evaluation parameters, such as energy consumption, algorithm complexity, etc., and analyze the SEK-based DSE scheme from more perspectives.

Finally, we would like to once again express our deepest gratitude to Reviewer 2 for your recognition, the time and effort you have dedicated, and the precious suggestions. And we look forward to improving the practicality and universality of our scheme and contributing more valuable research results in the field of IoT physical layer security with your continued support.

Dear Prof. Nei Kato,,

Thank you very much for your email on Jan. 10, 2025 and hard work for our manuscript of IoT-41406-2024 of "*A Physical Layer Endogenous Security Architecture with Dynamic Slicing Encryption for IoT*."

We also express our sincere thanks to Associate Editor: Dr. Mi Wen, and two Reviewers for their careful assessments and constructive comments, particularly for all of people to spend a lot of time to review our manuscript.

We cherish this opportunity for Mandatory Minor Revisions given by you, and have carefully read and understood all the comments. Over the past ten days, we have taken all comments into consideration, improve the entire manuscript, and completed the responding letter to all of the reviewer points carefully, including our modification description and point-by-point responses to the comments.

We hope the manuscript in this status can meet the criteria for publication in your esteemed journal. We now resubmit the revisions with following files:

1. The revised manuscript with highlights all changes in red is marked as "IoT-41406-2024-R1-red color";
2. The revised manuscript without any highlighting is marked as "IoT-41406-2024-R1-clear";
3. The Responding Letter document;
4. This cover letter to you.

The attached please the responding letter file.

With my best regards,

Xiaohan Sun
Professor and Director
National Research Center for Optical Sensing/Communications Integrated Networking
School of Electronics Science and Engineering
Southeast University
Nanjing 210096, China
Tel/Fax: +86-13851681227
Email: xhsun@seu.edu.cn