ITU Journal on Future and Evolving Technologies, Volume 4, Issue 1, March 2023

WIRELESS PHYSICAL-LAYER ENCRYPTION WITH PROGRAMMABLE METASURFACE IN REAL ENVIRONMENT

Menglin Wei[1], Zhuo Wang[1], Hanting Zhao[1], Tie Jun Cui[2], Lianlin Li[1]

[1]State Key Laboratory of Advanced Optical Communication Systems and Networks, School of Electronics, Peking University, Beijing 100871, China, [2]State Key Laboratory of Millimeter Waves, Southeast University, Nanjing 210096, China

NOTE: Corresponding authors: Lianlin Li, lianlin.li@pku.edu.cn and Tie Jun Cui, tjcui@seu.edu.cn

Abstract *– Wireless communication with physical layer security is of great importance in modern society, especially with the advent of the Internet-of-Things, fifth-generation communication, and beyond. More recently, metasurface-enabled physical-level encryption methods have attracted researchers' attention, in which the programmable metasurface is introduced as a controllable temporal entropy source. In this work, we present a novel approach to wireless physical-layer encryption by exploring the programmable metasurface as the high temporal-spatial entropy source via its unique capability in manipulating a flexibly temporal-spatial electromagnetic wavefront. We implement a proof-of-principle system working at around 2.4 GHz and develop associated efficient algorithms for the generation of a physical-level encryption key, where the programmable metasurface and surrounding environment are treated as a whole in a deterministic way. We experimentally demonstrate that the proposed method enables us to generate the Mbps-rate encryption key with the high spatial-temporal entropy in real-world settings. Our work could pave the way toward the next generation of model-free physical-layer secure wireless communication.*

Keywords – Physical-level encryption, programmable metasurface, secure wireless communication

1. INTRODUCTION

Wireless communication is a fundamental tool of information transfer in modern society [1]. However, it is vulnerable to eavesdropping due to its broadcasting feature, although various digital-layer encryption techniques have been developed by now. To deal with this formidable problem physical-layer encryption, pioneered by Maurer in 1993 [2], has been attracting ever-increasing interest [3], especially with the advent of the Internet-of-Things, and fifth-generation communication and beyond; and it relies on the 'fingerprint' of the physical time-varying wireless channel between legitimate parties, and explore it as the 'private' encryption key. Such an encryption strategy could enable us to achieve wireless communication with one-time-pad encryption [7] and is an attractive alternative to the digital public-key techniques. Over the past few years, we have witnessed that considerable effort has been made in the realm of physical-layer encryption. However, they are often limited to the low rate of encryption key due to the slowly varying channel conditions and are impractical in a real-world setting. To tackle this limitation, researchers and engineers have begun to explore the *artificial* wireless channels with programmable metasurfaces in physics or reconfigurable intelligent surfaces in communications [4-10], as opposed to the exploitation of wireless channels already existing in nature, to construct actively the controllable time-varying wireless channel for the generation of an encryption key. It is apparent that, to achieve the optimal or at least suboptimal performances of physical-level encryption, a fundamentally critical issue to them is how to deal with the coupling between the artificial wireless channel and the surrounding natural channel. By now, the artificial channel is pursued under a *statistical* model of the surrounding natural physical channel. Thereby, the metasurface is nearly independent of the specific surrounding environment, and thus the resultant physical-level encryption solutions are not optimal and leaves a lot of room for further improvement.

In this work, in order to address the above difficulty, we present a novel approach to wireless physical-level encryption by exploring the capability of programmable metasurfaces in manipulating flexibly the Electromagnetic (EM) spatial-temporal wavefront. The programmable metasurface is an ultrathin array of controllable manmade elements (i.e., meta-atoms) [11-14], and has found many valuable applications in sensing [15-19], communications [20-22], analog computing [23], and others [24]. In the community of physical-level encryption, the programmable metasurface was usually utilized as an entropy source for the generation of a physical-level encryption key, where the metasurface is controlled to match *statistically* with a certain type of surrounding environment, rather than match *deterministically* with the underlying specific surrounding environment. Note that the state-of-art switching speed of a moderate-size programmable metasurface is in the order of MHz per pattern or faster [21, 22]. We denote by the pattern the control coding sequence of the metasurface. In this work, taking this fact into account, we present the wireless physical-level encryption method, which controls the metasurface to be *deterministically* consistent with the specific physical environment in a real-time way. Then, the physical-level encryption key can be generated at the rate of Mbps, and can be transferred to the intended user(s) simultaneously through the powerful beam-forming ability of the programmable metasurface, sharing a similar operational mechanism with metasurface-enabled backscattering communication [25]. Compared with existing metasurface-enabled wireless physical-level encryption methods, the metasurface here is not only used as the high-capacity temporal entropy source for the physical-level encryption key generation, but also as the high-capacity beam-forming device for the secret wireless key transfer on the physical level. The paper contains the following contributions:

- We present a novel method for physical-layer wireless secret key generation and transmit it with a programmable metasurface in a real-world setting. Here, the rate of encryption keys is fast in the order of Mbps, even in a static propagation environment.
- We develop an efficient online search algorithm of the coding pattern of the metasurface so that the metasurface is deterministically consistent with the underlying physical environment.
- We implement a proof-of-concept system working at around 2.4 GHz and verify experimentally its superior performance.

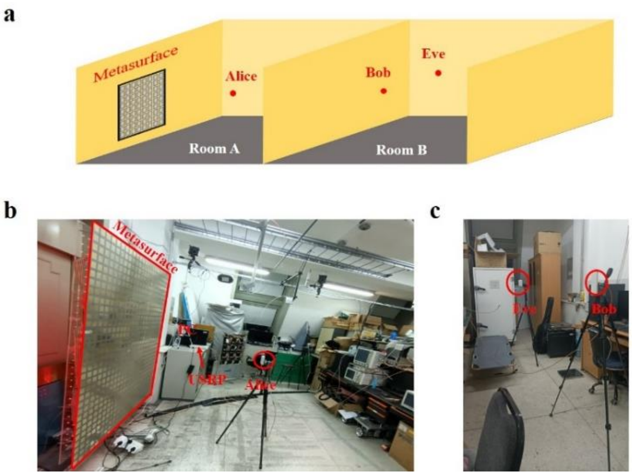

Fig. 1 – Experimental configuration of the proposed metasurface-enabled wireless physical-level encryption. (a) The sketch map of experimental setting, where Alice and Bob are the legitimate users, Eve is an eavesdropper. Additionally, a programmable metasurface with a size of 1.7 m by 1.3 m is deployed in Room A. In our experiments, a commercial software defined device, i.e., USRP X310, is utilized to launch and acquire radio signals. (b) Picture of experimental setting in room A, where the programmable metasurface has been marked in a red square. (c) Picture of experimental setting in room B

2. MODELS AND METHODS

2.1 System model

The system model of the proposed metasurface-enabled wireless physical-level encryption is sketched in Fig. 1a, where Alice and Bob are legitimate users, and they aim to extract the secret key from the wireless channel of the metasurface-embedded physical environment. In addition, Eve is a passive eavesdropper who wants to eavesdrop on Alice's data. In the metasurface-embedded physical environment, the time-varying Alice-Bob's channel response can be modelled as:

$$h_{BA}(t) = G(\boldsymbol{r}_B, \boldsymbol{r}_A; t) + \sum_{n=1}^{N} \alpha_n(t) G(\boldsymbol{r}_n, \boldsymbol{r}_A; t) G(\boldsymbol{r}_B, \boldsymbol{r}_n; t), \qquad (1)$$

Here, the time t reflects the change of the wireless channel, which is slow in scale with respect to the time-domain radio signal, and thus is referred as the slow time. In Eq. 1, $G(\boldsymbol{r}_B, \boldsymbol{r}_A; t)$ is the so-called Green's function of the surrounding physical environment, which describes the electromagnetic response at $\boldsymbol{r}_B$ arising from a point source at $\boldsymbol{r}_A$ [19]. In addition, $\boldsymbol{r}_n$ and $\alpha_n \in \{1, -1\}$ are the spatial location and the reflection coefficient of the nth meta-atom, respectively, $\boldsymbol{r}_B$ and $\boldsymbol{r}_A$ are spatial locations of Bob and Alice, respectively.

The metasurface is assumed to be composed of N independently controllable one-bit meta-atoms, and, for simplicity, each meta-atom has the isotropic radiation pattern. Similar to Eq. (1), the Alice-Eve's channel response reads:

$$h_{EA}(t) = G(\boldsymbol{r}_E, \boldsymbol{r}_A; t) + \sum_{n=1}^{N} \alpha_n(t) G(\boldsymbol{r}_n, \boldsymbol{r}_A; t) G(\boldsymbol{r}_E, \boldsymbol{r}_n; t) \qquad (2)$$

In a nutshell, the discrete time sequence of $h_{BA}(t)$ is explored as the encryption key. Here, we would like to emphasize two basic criteria for the physical-level encryption key: (1) the sequence of $h_{BA}(t)$ needs to have the temporal entropy as big as possible, i.e., is fast varying in slow time, ensuring the fast-rate encryption key. (2) the sequence of $h_{BA}(t)$ needs to be a unique finger to the legitimate users, i.e., Alice and Bob, implying that it should be as incoherent with the sequence of $h_{EA}(t)$ as possible. It is worth pointing out that since the programmable metasurface is utilized to be rapidly switched in the order of μs, the channel response of the surrounding environment is unchanged largely and is approximately static. It is well known that the programmable metasurface is capable of flexibly manipulating the temporal-spatial EM wavefront on the physical level, implying that the physical radiation pattern of a programmable metasurface has large entropies in both the temporal and spatial domain. Therefore, a programmable metasurface with proper control can be explored as a good candidate for the large-entropy wireless physical-level encryption with big entropy. To this end, it is of critical importance to finalize an optimal control pattern of the metasurface in the given surrounding environment, as implied in Eq. 1 and Eq. 2. However, it remains challenging mainly because the Green's function in a real-world environment is hard to obtain. To deal with this difficulty, an online search algorithm has been proposed in this work, which is detailed in the next section. After achieving the channel response, the encryption key can be easily achieved through some standard steps including quantizing, information reconciliation and privacy amplification, which is similar to conventional methods.

2.2 Design of programmable metasurface

The programmable metasurface utilized in this work is the same as that in [17], which was developed in our group. For readers' convenience, some details about it are briefly presented below. The programmable metasurface is composed of independently-controllable 32 × 24 meta-atoms, and has a size of 1.7 × 1.3 m^2 in total, as shown in Fig. 1b for the front view of the metasurface. Each meta-atom with the size of 54 × 54 mm^2 is integrated with an SMP1345-079LF PIN diode. We experimentally observe that the reflection phase of the meta-atom experiences a 180° phase difference when the PIN diode is switched from ON (OFF) to OFF (ON) in the frequency range of 2.41-2.48 GHz. The phase change can be accomplished by switching the external DC voltage applied to the PIN diode from 3.3 V to 0 V. We remark that the whole metasurface is composed of 4 × 3 identical panels due to the restriction of fabrication, and each panel has 8 × 8 meta-atoms. Each metasurface panel is equipped with eight 8-bit shift registers (SN74LV595APW), and every 8 PIN diodes share the same shift register. With the use of shift registers, 8 PIN diodes are sequentially controlled. Then an FPGA-based Micro-Control Unit (MCU) will send the commands over 24 independent branch channels, leading to almost real-time manipulations of all PIN diodes. The whole programmable metasurface is electronically controlled with an MCU. An FPGA chip is used to distribute all commands to 768 PIN diodes. To achieve the real-time and flexible controls of 768 PIN diodes soldered in the programmable metasurface, an MCU with a size of 95 × 145 mm^2 is designed and assembled on the upper rear of the metasurface. The MCU is responsible for dispatching all commands sent from a master computer subject to one common clock (CLK) signal. In our work, the adopted CLK is 100 MHz, and the switching time of the PIN diode is about 1μs each cycle.

2.3 Online search algorithm for the coding pattern of the programmable metasurface

Here, we elaborate on the efficient solution of the binary coding pattern of the metasurface in the temporal-spatial domain. Conventionally, the aforementioned Green's function has been treated in a *statistical* way, which is assigned with a certain type of parameterized probability distribution [4-10]. In this way, the optimized metasurface coding pattern is nearly independent of the specific surrounding environment, and thus the resultant encryption performance is usually not optimal. As opposed to this kind of approach, we deal with the Green's function in a deterministic manner, implying that the programmable metasurface is designed to match with the physical surrounding metasurface in a deterministic way. Thereby, it can be expected that the encryption performance will be remarkably improved compared with existing similar methods.

Typically, the Green's function for the complicated physical environment is unknown, therefore there is no analytical representation available. To deal with this difficulty, we develop an online search algorithm. In nutshell, the online search algorithm is to find the optimal states of the metasurface's meta-atoms in a trial-and-decision manner. In particular, a set of neighboured meta-atoms are randomly chosen and their states are changed to be opposite, and check whether the resultant beam's amplitude is increased with respect to that without the changes of the chosen meta-atoms. If the beam's amplitude goes up, then the states of the chosen meta-atoms are kept; otherwise, give up this choice. Repeat this procedure, until the beam's amplitude is convergent to a stable value. More details about the amplitude-only online search algorithm are summarized below.

Algorithm 1. Amplitude-only online searching algorithm for the optimal binary coding pattern $\mathbf{\Phi}_0$

```
Initialization:

Set the above G-S solution for the initial coding pattern $\mathbf{\Phi}_0$, and then acquire the signal's amplitude $A_0^j$ (j=1, 2, ..., J) at the intended location, where $j$ is for the $j$th radiation beam, and $J$ is the number of beams in total.

WHILE (DC$(A_k^j, A_{k-1}^j) > \epsilon$, j=1, 2, ..., J)
    DO i=1:768
        1) Choose randomly a set of $2 \times 2$ neighbored meta-atoms, change their states to be opposite, and arrive at a new coding pattern $\mathbf{\Phi}$.
        2) Acquire the signal's amplitudes: $\{A^j, j = 1, 2, \dots, J\}$.
        3) If DC$(A^j, A_{k-1}^j) > 0$ (j=1, 2, ..., J), then $A_k^j = A^j$ (j=1, 2, ..., J), $\mathbf{\Phi}_k = \mathbf{\Phi}$ and $k = k + 1$.
    END DO
END WHILE
```

Herein, we introduce a decision criterion $\mathrm{DC}(A_k^j, A_{k-1}^j) = A_k^j - A_{k-1}^j$. In addition, ϵ is a stop threshold, and we set it as 0.001 in our implementation.

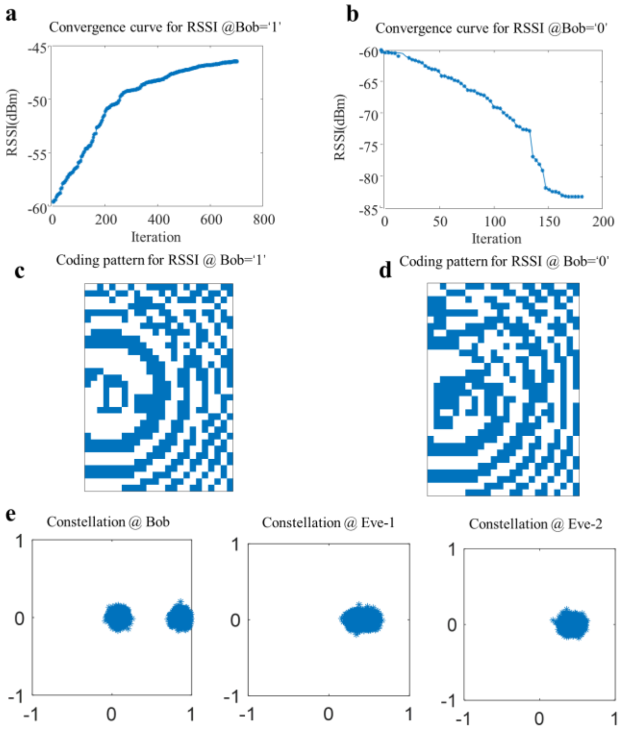

Fig. 2 – Experimental results of RSSI-based physical-level encryption with our demo system. (a)-(b) The dependencies of the RSSI as the growth of iterations for the wireless channel states '1' and '0', respectively. (c)-(d) The optimized patterns of the metasurface corresponding to (a) and (b), respectively. (e) The constellations obtained at Bob, Eve-1 and Eve-2 from left to right in order

3. RESULTS AND DISCUSSION

We implement two groups of experimental results to demonstrate the performance of the proposed metasurface-enabled wireless physical-level encryption method, where the Received Signal Strength Indication (RSSI) and Channel State Information (CSI) of the hybrid wireless channel are considered, respectively. As shown in Fig. 1a, Alice and Bob are a pair of legitimate users, and they aim to extract the secret key from the hybrid wireless channel of the metasurface-embedded physical environment. The legitimate users, Alice and Bob locate at $(-0.1\text{ m}, 0, 1.2\text{ m})$ and $(0.2\text{ m}, -1.2\text{ m}, 4.1\text{ m})$, respectively; meanwhile, two eavesdroppers, Eve-1 and Eve-2 sit at $(0.3\text{ m}, -2.6\text{ m}, 4.3\text{ m})$ and $(0.2\text{ m}, 2.2\text{ m}, 1.6\text{ m})$, respectively. In our implementation, the radio signals are generated and acquired using the Ettus USRP X310.

Case Study 1. RSSI-based wireless physical-level encryption

We examine the performance of our metasurface-enabled wireless physical-level encryption method, where the RSSI of a hybrid wireless channel is explored for the generation of a physical-level encryption key. For simplicity, we consider that the hybrid wireless channel is designed to have two RSSI states, denoted as ‘1’, and ‘0’. For this reason, we would like to refer to this kind of channel as the Binary Amplitude Shifting Key channel (*BASK channel* in short). In order to achieve the encryption key on the physical level, we need to control the programmable metasurface so that the optimized hybrid wireless channel has two distinguishable RSSI states: high-level and low-level, which are characterized with binary digits ‘1’ and ‘0’, respectively. To this end, two corresponding coding patterns of the programmable metasurface are required. In light of the online search algorithm outlined previously, Bob is asked to emit first a series of probing signals (2.442 GHz monochromic continuous wave is considered here). Meanwhile, Alice acquires the RSSI and adjusts in situ the coding pattern of the metasurface until the maximum (or minimum) RSSI is achieved, respectively. Figures 2a and 2b report the dependencies of the RSSI as the growth of iterations for the wireless channel states ‘1’ and ‘0’, respectively. Correspondingly, the optimized coding patterns of the metasurface are shown in Fig. 2c and d, respectively. It can be observed that the high-level and low-level RSSI achievable are around −46 dBm and −83 dBm, respectively, which are distinguishable for a usual commodity detector. That is to say, the optimized hybrid wireless channel has two distinct RSSI states for the legitimate users of Alice and Bob. In order to show the unique ‘finger’, or ‘security’ of the achieved channel for the legitimate users, we present the constellations obtained at Bob, Eve-1 and Eve-2 in Fig. 2e. Apparently, we can see that Bob can easily detect the encryption key from Alice, but Eve-1 and Eve-2 fail to do this job.

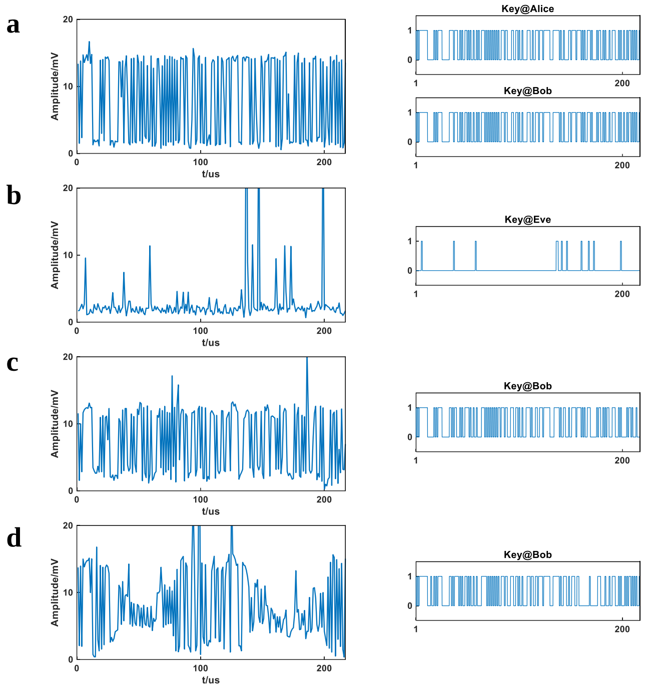

Fig. 3 – Experimental results of RSSI-based physical-level encryption key. (a) The encryption key decoded at Bob. (left) a 217 µs-length RSSIs at Bob, and (right) the first 217 decoded bits at Alice (top) and Bob (bottom). (b) The encryption key decoded at Eve. (left) a 217µs-length RSSIs at Eve, and (right) the first 217 decoded bits at Eve. (c)-(d) Corresponding results at Bob, but a person and two people are asked to walk freely in room B

Now, we turn to discuss the rate of the metasurface-enabled encryption key with our proof-of-concept system. To this end, a set of experiments are conducted and corresponding results are presented in the first row of Fig. 3. Recall that such RSSIs are used for the encryption key. A 217 µs-length RSSI received at Bob and the corresponding first 217 decoded bits are shown in the left and right of the first row of Fig. 3a, where the bitstream emitted by Alice is also shown. It can be seen that the key rate that our system can achieve is in the order of Mbps, which benefits from the fast-switching speed of the designed programmable metasurface in µs per pattern. Of course, the key rate can be further increased by designing a more specialized programmable metasurface. For comparison, the corresponding results at Eve are shown in Fig. 3b. Further, in order to examine the robustness of the encryption key to the changing environment, we have conducted another two sets of experiments, where a person and two people walk freely in room B, and corresponding experimental results are shown in the third and bottom rows of Fig. 3. It can be seen that the metasurface-enabled physical-level encryption key from Alice can be well recognized by Bob in a robust way, which does make sense because the encryption key is transferred from Alice to Bob in a point-to-point manner owing to the powerful beam-forming capability of the programmable metasurface. To summarize, we can conclude from the above results that the fast-rate encryption key is unique and robust to the legitimate users of Alice and Bob. That is to say, the legitimate user Bob can robustly capture the encryption key from Alice, but the eavesdropper Eve fails to do it.

Case study 2. CSI-based wireless physical-level encryption

Physical-level encryption key based on RSSI is susceptible to additive noise pollution resulting in a bad bit error rate. At the same time, it is difficult to fight against Eve with high SNR located near Bob. To address this problem, we consider exploring the CSI information of the metasurface-embedded wireless channel for the generation of a physical-level encryption key. To that end, several experiments have been conducted, where the experimental setting here is the same as that used in the RSSI case. In addition, for simplicity, we attempt to manipulate the metasurface so that the hybrid wireless channel has two opposite phase states: 0 and π, which are characterized by binary digits ‘0’ and ‘1’, respectively. For notation convenience, we refer to this kind of hybrid wireless channel as the Binary Phase Shifting Key channel (*BPSK channel* in short) in this work. Of course this method can be generalized into that with multiple-level phase states in a straightforward way. Similar to the above, we need to find two coding patterns of the metasurface; however, the online search algorithm outlined above is limited to the RSSI case (i.e., intensity alone) and is not directly applicable to the CSI case requiring the intensity plus phase. In order to address this problem, we implement the online search algorithm multiple times with different initial solutions and pick up two desired solutions among them. Fig. 4a reports the dependencies of the RSSI as a function of iterations for the BPSK channel, where the blue and yellow lines correspond to the hybrid wireless channel with the phase responses of 0 and π , respectively. The optimized coding patterns of the metasurface are shown in Fig. 4c and 4d for the 0 and π channels, respectively. Note that these two channels have the opposite phase states but nearly identical RSSIs. Thereby, the optimized hybrid wireless channel has two distinct CSI states for the legitimate users of Alice and Bob. To demonstrate the ‘security’ of the achieved BPSK channel for the legitimate users we present the constellations obtained at Bob, Eve-1 and Eve-2 in Fig. 4e. Apparently, we can see that Bob can easily detect the encryption key from Alice, but Eve-1 and Eve-2 fail to do this job.

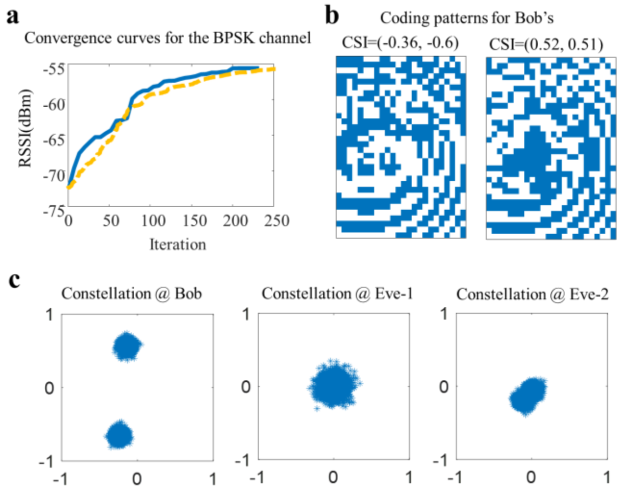

Fig. 4 – Experimental results of CSI-based physical-level encryption with our demo system. (a) The dependencies of the RSSI as the growth of iterations for the BPSK wireless channel states, where the blue and yellow lines correspond to the channel states ‘1’ and ‘0’, respectively. (b)The optimized patterns of the metasurface corresponding to the states of BPSK wireless channel ‘0’ and ‘1’, respectively. (c) The constellations obtained at Bob, Eve-1 and Eve-2 from left to right in order

Now, we discuss experimentally the key rate of the CSI-based physical-level encryption with our proof-of-concept system. Experimental results are presented in the first row of Fig. 5. Here, the metasurface is dynamically manipulated so that the desired time-varying CSIs of the hybrid wireless channel are for the legitimate users, i.e., a 217 μs-length amplitude and phase of CSIs received at Bob and the corresponding first 217 decoded bits are shown in the left of the first row of Fig. 5a, where the BPSK bit stream emitted by Alice is shown. For comparison, the corresponding results at Eve are shown in Fig. 5b. In addition, we have conducted another two sets of experiments, where a person and two people walk freely in room B, and corresponding experimental results are shown in the third and bottom rows of Fig. 5. Similar to the RSSI case, we can observe from the above experimental results that the encryption key with the rate of Mbps can be achieved on the physical level by controlling actively the CSI information of the metasurface-embedded wireless channel.

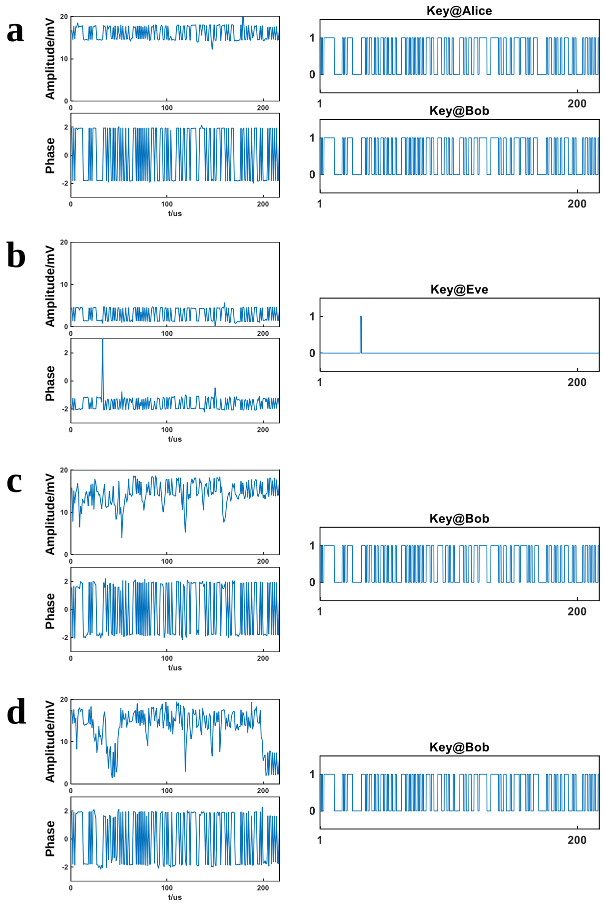

Fig. 5 – Experimental results of CSI-based physical-level encryption key. (a) The encryption key decoded at Bob. (left) a 217 μs-length CSIs at Bob, and (right) the first 217 decoded bits at Alice (top) and Bob (bottom). (b) The encryption key decoded at Eve. (left) a 217 μs-length CSI at Eve, and (right) the first 217 decoded bits at Eve. (c)-(d) Corresponding results at Bob, but a person and two people are asked to walk freely in room B

4. CONCLUSION

To summarize, we present a novel approach to the wireless physical-layer encryption by exploring the inexpensive programmable metasurface as the big temporal-spatial entropy source due to its unique capability in manipulating a flexibly temporal-spatial electromagnetic wavefront. We implement a proof-of-principle system working at around 2.4 GHz and design the associated algorithms for the generation of a physical-level encryption key. Moreover, we propose an online search algorithm to find the coding pattern of the programmable metasurface. Being sharply different from existing metasurface-enabled encryption methods, the proposed method deals with the programmable metasurface and the surrounding physical environment as a whole in a deterministic manner, which is responsible for the physical-level wireless encryption key with the high temporal-spatial entropy. To illustrate this principle, we consider two hybrid wireless channels, i.e., BPSK channel and BASK channel, and experimentally demonstrate that the fast-rate encryption key achieved is unique and robust to the legitimate users on the physical level. Our work could pave a novel way towards the next generation of model-free physical-layer secure wireless communication.

REFERENCES

[1] Goldsmith, A. Wireless Communications. (Cambridge University Press, 2005).

[2] U. M. Maurer. Secret key agreement by public discussion from common information. *IEEE Trans. Info. Theory*, 39(3):733–742(1993).

[3] S. Mathur, W. Trappe, N. Mandayam, et al., Radio-telepathy: extracting a secret key from an unauthenticated wireless channel, *MobiCom'08,* September 14–19, 2008, San Francisco, California, USA (2008).

[4] L. Yang, J. Yang, W. Xie, et al., Secrecy performance analysis of RIS-aided wireless communication systems, IEEE Trans. Vehicular Technology, 69, 10, 12296-12300 (2020).

[5] J. Qiao and M.-S. Alouini, Secure transmission for intelligent reflecting surface-assisted mmWave and Terahertz systems, IEEE Wireless Communication Letters, 9, 10, 1743-1747 (2020).

[6] X. Lu, J. Lei, Y. Shi, et al., Intelligent reflecting surface assisted secret key generation, IEEE Signal Processing Letters, 28, 1036-1040 (2021).

[7] X. Hu, L. Jin, K. Huang, et al., Intelligent reflecting surface-assisted secret key generation with discrete phase shifts in static environment, IEEE Wireless Communication Letters, 10, 9, 1867-1870 (2021).

[8] P. Staat, H. Elders-Boll, M. Heinrichs, Intelligent reflecting surface-assisted wireless key generation for low-entropy environments, 2021 IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), (2021).

[9] Z. Ji, P. L. Yeoh, G. Chen, et al., Random shifting intelligent reflecting surface for OTP encrypted data transmission, IEEE Wireless Communications Letters, 10, 6, 1192-1196 (2021).

[10] Z. Ji, P. L. Yeoh, D. Zhang, et al., Secret key generation for intelligent reflecting surface assisted wireless communication networks, IEEE Trans. Vehicular Technology, 70, 1, 1030-1034 (2021).

[11] Cui, T. J., Qi, M. Q., Wan, X., Zhao, J. & Cheng, Q. Coding metamaterials, digital metamaterials and programmable metamaterials. Light Sci. Appl. 3, e218–e218 (2014).

[12] Li, L. & Cui, T. J. Information metamaterials – from effective media to real-time information processing systems. Nanophotonics 8, 703-724 (2019).

[13] Y. Shuang, et al., One-bit quantization is good for programmable coding metasurfaces, 65, 172301: 1-15(2022).

[14] Ou, J.-Y., Plum, E., Zhang, J. & Zheludev, N. I. An electromechanically reconfigurable plasmonic metamaterial operating in the near-infrared. Nat. Nanotech. 8, 252–255 (2013).

[15] Watts, C. M. et al. Terahertz compressive imaging with metamaterial spatial light modulators. Nat. Photonics 8, 605–609 (2014).

[16] Li, L. et al. Machine-learning reprogrammable metasurface imager. Nat. Commun. 10, 1082 (2019).

[17] Li, L. et al. Intelligent metasurface imager and recognizer. Light Sci. Appl. 8, 97 (2019).

[18] Li, H.-Y. et al. Intelligent Electromagnetic Sensing with Learnable Data Acquisition and Processing. Patterns 1, 100006 (2020).

[19] Li, L. et al. Electromagnetic reprogrammable coding-metasurface holograms. Nat. Commun. 8, 197 (2017).

[20] Renzo, M. D. et al. Smart radio environments empowered by reconfigurable AI meta-surfaces: an idea whose time has come. J. Wireless Com. Network 2019, 129 (2019).

[21] Zhang, L. et al. Space-time-coding digital metasurfaces. Nat. Commun. 9, 4334 (2018).

[22] H. Zhao et al., Metasurface-assisted massive backscatter wireless communication with commodity Wi-Fi signals. Nat. Commun. 11, 3926 (2020).

[23] del Hougne, P. & Lerosey, G. Leveraging Chaos for Wave-Based Analog Computation: Demonstration with Indoor Wireless Communication Signals. Phys. Rev. X 8, 041037 (2018).

[24] Kaina, N., Dupré, M., Lerosey, G. & Fink, M. Shaping complex microwave fields in reverberating media with binary tunable metasurfaces. Sci. Rep. 4, 6693 (2015).

[25] L. Li, Zhao H., Liu C., et al., Intelligent metasurfaces: control, communiation and computing, eLight, 2: 7 (2022).

AUTHORS

Menglin Wei is pursuing his Ph.D. degree in electromagnetic field and microwave technology from the School of Electronics, Peking Univeçrsity, Beijing, China. His current research interests include physical layer security, intelligent metasurface and intelligent sensing.

Zhuo Wang is currently working toward his Ph.D. degree in electromagnetic field and microwave technology from the School of Electronics, Peking University, Beijing, China. His research interest is intelligent electromagnetic sensing systems.

Hanting Zhao was born in Shandong, China, in 1996. He received a B.E. degree from the College of Electronic Information Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2019. He is currently pursuing a Ph.D. degree with the School of Electronics, Peking University, Beijing, China. He worked on various projects related to radio signal processing and novel electromagnetic wave manipulation systems. His current research interests include intelligent metasurface, passive electromagnetic imaging, passive metasurface based wireless communication and metasurface robotics.

Tie Jun Cui (Fellow, IEEE) received B.Sc., M.Sc., and Ph.D. degrees in electrical engineering from Xidian University, Xi'an, China, in 1987, 1990, and 1993, respectively. In March 1993, he joined the Department of Electromagnetic Engineering, Xidian University, where he was promoted to an associate professor in November 1993. From 1995 to 1997, he was a research fellow with the Institut für Hochstfrequenztechnik und Elektronik (IHE), University of Karlsruhe, Karlsruhe, Germany. In July 1997, he joined the Center for Computational Electromagnetics, Department of Electrical and Computer Engineering, University of Illinois at Urbana–Champaign, Champaign, IL, USA, first as a postdoctoral research associate and then as a research scientist. In September 2001, he was Cheung Kong professor with the Department of Radio Engineering, Southeast University, Nanjing, China. He is currently chief professor with Southeast University, director of the State Key Laboratory of Millimeter Waves, and founding director of the Institute of Electromagnetic Space, Southeast University. He proposed the concepts of digital coding and programmable metamaterials, and realized their first prototypes, based on which he founded the new direction of information metamaterials, bridging the physical world and digital world. He is the first author of books: Metamaterials: Theory, Design, and Applications (Springer, November 2009); Metamaterials: Beyond Crystals, Noncrystals, and Quasicrystals (CRC Press, March 2016); and Information Metamaterials (Cambridge University Press, 2021). He has published over 500 peer-reviewed journal articles, which have been cited by more than 44 600 times (H-factor 107; Google Scholar), and licensed over 100 patents. His research interests include metamaterials and computational electromagnetics.

Dr. Cui was awarded a research fellowship from the Alexander von Humboldt Foundation, Bonn, Germany, in 1995. He received the Young Scientist Award from the International Union of Radio Science in 1999; the Cheung Kong Professor by the Ministry of Education, China, in 2001; the National Science Foundation of China for Distinguished Young Scholars in 2002; the Natural Science Award (First Class) from the Ministry of Education, China, in 2011; and the National Natural Science Awards of China (Second Class, twice) in 2014 and 2018. His research has been selected as one of the most exciting peer-reviewed optics research "Optics in 2016" by Optics and Photonics News Magazine, 10 Breakthroughs of China Science in 2010, and many research highlights in a series of journals. His work has been widely reported by Nature News, MIT Technology Review, Scientific American, New Scientists, Discover, and so on. He is the academician of the Chinese Academy of Science. He served as an associate editor for IEEE Transactions on geoscience and remote sensing, and as a guest editor for Science China Information Sciences, Science Bulletin, and for IEEE Journal on emerging and selected topics in circuits and systems, engineering, and research. He is also the chief editor of Metamaterial Short Book Series in Cambridge University Press, an editor of Materials Today Electronics, an associate editor of Research, and an editorial board member of National Science Review, eLight, PhotoniX, Advanced Optical Materials, Small Structures, and Advanced Photonics Research. He presented more than 100 keynote and plenary talks in academic conferences, symposiums, and workshops. From 2019 to 2021, he was ranked in the top 1% for the highly cited papers in the field of physics by Clarivate Web of Science (Highly Cited Researcher).

Lianlin Li is a professor and doctoral supervisor of School of Electronics, Peking University. In recent years, he has been engaged in research of electromagnetic sensing systems, algorithm and engineering applications. As first or corresponding author, he has published more than 80 papers in Nature Communications, Advanced Science, IEEE, etc., and published two academic monographs. Some of his research results have been applied in ionospheric exploration, oil exploration and wireless communication.