Research Article

Zhen Gu, Rensheng Xie, Haoyang Liu, Yiting Liu, Xiong Wang, Hualiang Zhang, Jianjun Gao, Liming Si*, Shuqi Chen and Jun Ding*

Dual-band complex-amplitude metasurface empowered high security cryptography with ultra-massive encodable patterns

https://doi.org/10.1515/nanoph-2024-0314
Received June 15, 2024; accepted July 7, 2024;
published online July 24, 2024

Abstract: The significance of a cryptograph method lies in its ability to provide high fidelity, high security, and large capacity. The emergence of metasurface-empowered cryptography offers a promising alternative due to its unparalleled wavefront modulation capabilities and easy integration with traditional schemes. However, the majority of reported strategies suffer from limited capacity as a result of restricted independent information channels. In this study, we present a novel method of cryptography that utilizes a dual-band complex-amplitude meta-hologram. The method allows for the encoding of 2^{25} different patterns by combining a modified visual secret-sharing scheme (VSS) and a one-time-pad private key. The use of complex-amplitude modulation and the modified VSS enhances the quality and fidelity of the decrypted results. Moreover, the transmission of the private key through a separate mechanism can greatly heighten the security, and different patterns can be generated simply by altering the private key. To demonstrate the feasibility of our approach, we design, fabricate, and characterize a meta-hologram prototype. The measured results are in good agreement with the numerical ones and the design objectives. Our proposed strategy offers high security, ultra-capacity, and high fidelity, making it highly promising for applications in information encryption and anti-counterfeiting.

Keywords: cryptography; ultra-capacity; dual-band meta-hologram; complex-amplitude modulation; information security

***Corresponding authors: Liming Si**, Beijing Key Laboratory of Millimeter Wave and Terahertz Technology, School of Integrated Circuits and Electronics, Beijing Institute of Technology, Beijing 100081, China,
E-mail: lms@bit.edu.cn; **Jun Ding**, Shanghai Key Laboratory of Multidimensional Information Processing, Key Laboratory of Polar Materials and Devices, East China Normal University, Shanghai 200241, China,
E-mail: jding@ee.ecnu.edu.cn
Zhen Gu and Jianjun Gao, Shanghai Key Laboratory of Multidimensional Information Processing, Key Laboratory of Polar Materials and Devices, East China Normal University, Shanghai 200241, China.
https://orcid.org/0000-0001-5103-7354 (Z. Gu)
Rensheng Xie, Department of Broadband Communication, Peng Cheng Laboratory, Shenzhen 518108, China.
https://orcid.org/0000-0003-0015-4571
Haoyang Liu and Xiong Wang, School of Information Science and Technology, ShanghaiTech University, Shanghai 201210, China.
https://orcid.org/0000-0001-9193-8181 (X. Wang)
Yiting Liu, The College of Engineering, Computing and Cybernetics, Australian National University, Canberra, ACT 2601, Australia
Hualiang Zhang, Department of Electrical and Computer Engineering, University of Massachusetts Lowell, Lowell, MA 01854, USA
Shuqi Chen, The Key Laboratory of Weak Light Nonlinear Photonics, Ministry of Education, School of Physics and TEDA Institute of Applied Physics, Nankai University, Tianjin 300071, China,
E-mail: schen@nankai.edu.cn. https://orcid.org/0000-0002-7898-4148

1 Introduction

Information security is of vital importance in modern wireless communications. Numerous information cryptography techniques have been investigated to attain a high level of security [1]–[5]. Among these, the benefits of metasurface-empowered cryptography, which allows for unprecedented manipulation of electromagnetic waves with multiple degrees of freedom (DoFs) (e.g., wavelength, polarization, phase, amplitude, etc.) [6]–[48], open up a new path for high security and large capacity. For instance, the wavelength can be used as a key for encryption, and the secret message can be obtained at the predetermined wavelength [6]. Using polarization as the key is another popular tactic [7]–[11]. By selecting the preset input and output polarization combinations, a 12-channel metasurface has been demonstrated [7]. Apart from the polarization-multiplexed encryption, the incident field modulated technology has also been employed for encryption [12], [13]. A re-programmable meta-hologram

is demonstrated for encryption with a high security level, where the secret message can only be extracted with a specific phase-modulated laser beam [13]. However, the secret message could be decrypted when a hacker intercepts all channel information in the aforementioned encryption methods. To tackle this issue, the metasurface-based encryption techniques that combine several DoFs have gained more attention. The utilization of multiple DoFs can not only greatly enhance the information capacity, but also raise the information security level by making the decryption key more complex [20]–[32].

Moreover, the VSS is a common computational imaging scheme that has been employed to metasurface-based cryptographies for improving the security of the secret message [34]–[36]. Polarization is used as the key in a theoretical demonstration of a secret-shared encoding technique based on the VSS [34]. In addition, to improve the storage of the encryption method without adding more channels, an encryption scheme by using one-time-pad key is proposed to generate 16 distinct images [35]. Although the security level could be increased by using the VSS-based methods, part of the fidelity is lost in the decrypted results, and the storage capacity is not large enough. In addition, by combining the holographic technology with the single-pixel imaging technology, an encryption method based on spatially multiplexed metasurface is demonstrated to include 26 letters and 10 numbers [33]. However, the number of unique symbols that can be encrypted by this method is determined by the metasurface size. Thus, it is highly demanded to develop a new cryptography approach that can encode a vast number of different symbols without requiring a large number of channels, while also ensuring the security and fidelity of the secret message as well as enabling dynamic adjustment of them.

In this work, we propose a novel cryptography method based on a dual-band complex-amplitude metasurface, which could encode 2^{25} different patterns or symbols. In the encryption phase, a cipher image is generated by extracting the features of the 2^{25} different patterns, which is transformed to the two frequency-selective shared keys (SKs) using the modified VSS scheme and a private key for each symbol in the secret message is converted to a 25-bit intensity sequence. Additionally, the two SKs are transformed to amplitude and phase distributions by the Gerchberg-Saxton (GS) algorithm, which are then recoded into a dual-band complex-amplitude metasurface. During the decryption phase, the two SKs represented by two holographic images can be reconstructed under a circularly polarized incidence, and the private key is received from a wireless channel. A cipher image is reconstructed by first performing an "XNOR" operation on the two SKs, and the secret symbol can be decrypted by further performing an "XOR" operation on the cipher image and the private key. Because each private key corresponding to a distinct symbol, this method is also known as a one-time-pad encryption method, which is theoretically unbreakable. Moreover, different message can be transmitted with the same metasurface by simply alternating the private keys, enabling dynamic adjusting of message. In this work, we only need to transmit the private key (i.e., a 25-bit binary intensity sequence) in the wireless channel. The SK_1 and SK_2 are transmitted by the meta-hologram, which can be reconstructed at a pre-set image plane under the correct incidence. By using the modified VSS and the one-time-pad encryption method, the proposed cryptography method features a much higher fidelity and could achieve ultra-massive encodable patterns with a higher security level, showcasing significant potential for advanced data storage and encryption.

2 Results and discussion

2.1 Operating principle and metasurface design

Figure 1 shows the schematic diagram of the proposed cryptography technique, which assumes that Bill wants to send a message to Donna. At the transmitting end, two SKs are encoded into a dual-band metasurface with complex-amplitude modulation. In addition, each symbol in the message is transformed into a private key as a 25-bit binary intensity sequence, which is then sent from a wireless channel. Moreover, this process so called "one-time-pad" encryption method allows the encoded message to be modified simply by altering the transmitted private keys, which could unbreakable [35]. At the receiving end, two holographic images SK_1 and SK_2 are reconstructed at frequencies f_1 and f_2, respectively, and an oscilloscope is used to receive the intensity signals (i.e., private keys). Then, Donna can superimpose the two SKs to generate the cipher image, and then decipher the message symbol by symbol through superimposing the private key sequence according to the decoding mechanism. Moreover, even if both the SKs and the private keys are intercepted (note: this is difficult due to the different encoding mechanisms and transmitting channels), the message cannot be deciphered without obtaining the decoding mechanism.

As an illustrative example, Figure 2(a) depicts a dual-band complex-amplitude meta-atom, which is composed of two metallic layers printed on opposing surfaces of an F4B dielectric substrate ($\varepsilon_r = 2.2$, $\tan\delta = 0.001$).

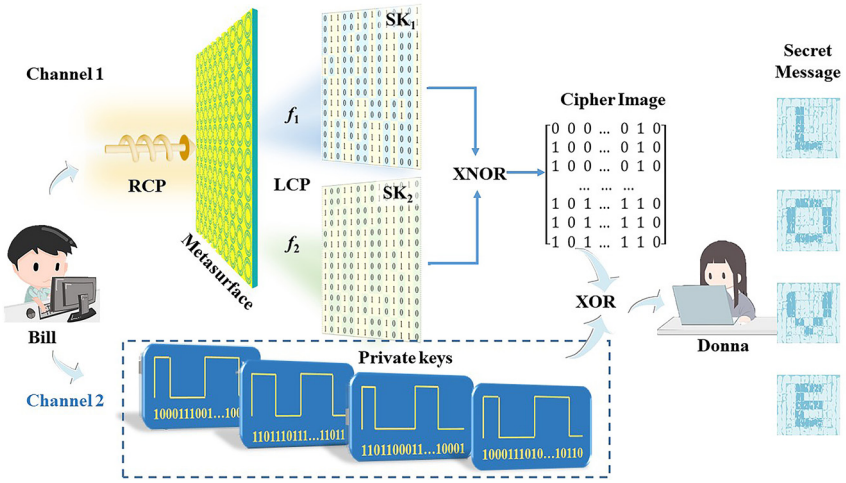

Figure 1: The schematic diagram of the proposed cryptography method.

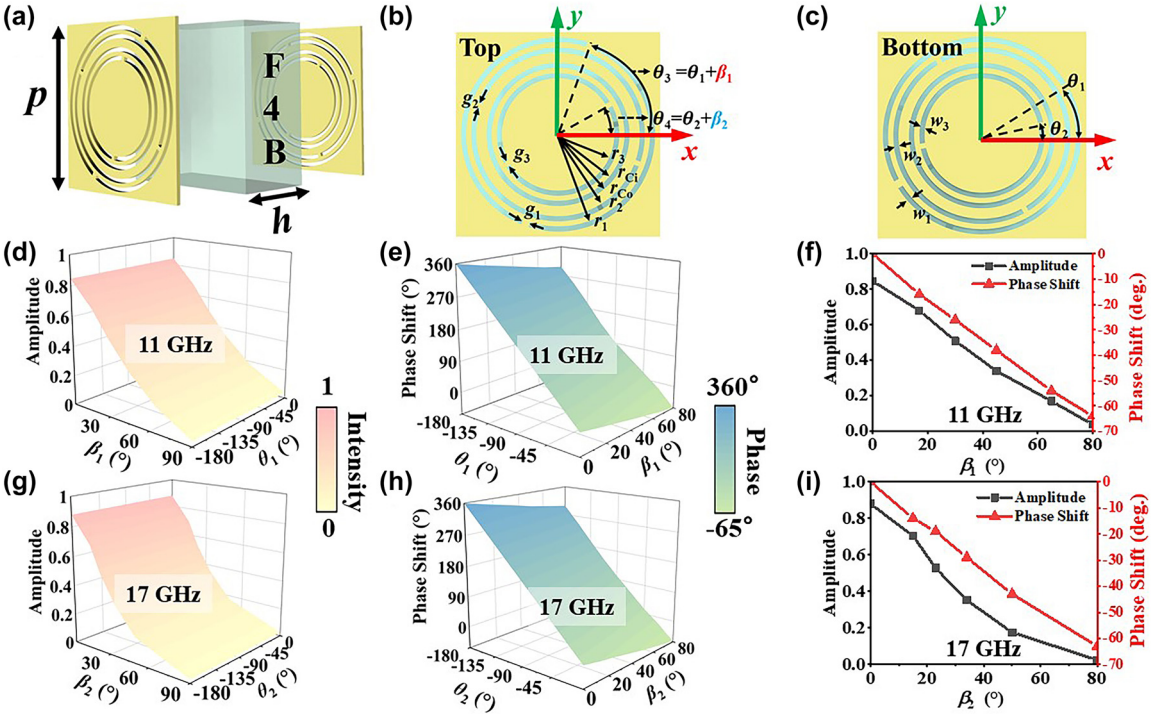

Figure 2: The proposed complex-ampliude meta-atom and their simulated amplitude and phase response. (a) The three-dimensional view, (b) top view, and (c) bottom view of the proposed complex-amplitude meta-atom. Specifically, $p = 8$, $h = 4$, $g_1 = 0.3$, $g_2 = 0.2$, $g_3 = 0.2$, $w_1 = 0.2$, $w_2 = 0.2$, $w_3 = 0.2$, $r_1 = 3.6$, $r_2 = 3.2$, $r_{Co} = 2.8$, $r_{Ci} = 2.6$, $r_3 = 2.2$ (unit: mm). (d) The amplitude and (e) phase shift compared with (0°, 0°) orientated meta-atom as functions of β_1 and θ_1 are presented at 11 GHz. (f) The amplitude and phase response with varied rotation angle β_1 at 11 GHz. (g) The amplitude and (h) phase shift compared with (0°, 0°) orientated meta-atom as functions of β_2 and θ_2 are presented at 17 GHz. (i) The amplitude and phase with varied rotation angle β_2 at 17 GHz.

Figure 2(b) and (c) plot the top and bottom metallic layers, consisting of a modified complementary split-ring resonator (MCSRR) and a modified double-C-slot resonator (MDCSR) located at the center. It is worth mentioning that the top and bottom layers have identical physical dimensions except for the orientation angles of the resonators. The orientation angles of the MCSRR and MDCSR denoted as θ_1 (θ_3) and θ_2 (θ_4) on the bottom (top) layer are defined as the angle between their incision gaps and the x-axis, respectively. The orientation angle difference between the MCSRRs (MDCSRs) on the top and bottom metallic layers is denoted as $\beta_1 = \theta_3 - \theta_1$ ($\beta_2 = \theta_4 - \theta_2$). During the meta-atom design process,

full-wave simulations were conducted by employing CST Microwave Studio, where the unit-cell boundary conditions were applied in both the *x*- and *y*-directions. The meta-atom was illuminated under a normal right-handed circularly polarized (RCP) incidence, and the phase and amplitude responses can be extracted by recording the transmitted left-handed circularly polarized (LCP) wave.

The simulated amplitude and phase responses by varying β_1 and θ_1 at 11 GHz are plotted in Figure 2(d) and (e), respectively. Figure 2(d) shows that the continuous amplitude modulation from 0 to a maximum, while Figure 2(e) demonstrates the whole 2π phase modulation. It can be seen from Figure 2(d) that the amplitude only depends on β_1, which changes very little when θ_1 is varied. Moreover, Figure 2(e) illustrates that a little phase shift might be induced by varying either β_1 or θ_1. Similar conclusions can be drawn from Figure 2(g) and (h) at 17 GHz, indicating that the amplitude response depends only on β_2, and the phase response depends on both β_2 and θ_2. In general, both the amplitude and phase modulation can be realized at two preset frequencies by varying the θ_1 (θ_2) and β_1 (β_2). In addition, the phase controls of the proposed meta-atom at two operating frequencies are completely independent, which is shown in Section I in the Supporting Information. Furthermore, the simulated amplitude and phase responses by varying β_1 (β_2) at 11 GHz (17 GHz) are plotted in Figure 2(f) and (i), respectively, where θ_1 (θ_2) is fixed to be 0°. It can be observed that the amplitude varies from 0.88 (0.85) to 0 by increasing β_1 (β_2) from 0° to 80° at 11 GHz (17 GHz). The theory analysis of the complex-amplitude modulation can be found in Section I in the Supporting information. In addition, the phase response decreases as β_1 or β_2 increases, which can be compensated by varying the θ_1 (θ_2) with an additional value also detailed in this part.

2.2 Encryption method

The encryption procedure is illustrated in Figure 3(a)–(g), which includes five key steps: the modified VSS encoding, complex-amplitude modulating, metasurface recoding, encrypting to the private keys, and loading on the intensity signals. In order to achieve a large capacity, we select a 5×5 matrix to represent a distinct symbol, whereby a white pixel (black pixel) of the matrix element is assigned a value '1' ('0'). In this way, a total of 2^{25} different symbols can be encoded. Then, the features of the 2^{25} different patterns are extracted to create a cipher image as a 7×7 matrix, which is subsequently converted to the two frequency-selective SKs using the modified VSS scheme depicted in Figure 3(a) and (b). In order to avoid the edge loss of the reconstructed hologram affecting the decrypted result, only the middle 5×5 part of the 7×7 matrix in the cipher image contains the secret message. Moreover, the detailed comparison of the traditional and modified VSS schemes is demonstrated in Section II in the Supporting Information, which indicates a significantly higher level of fidelity for the modified VSS

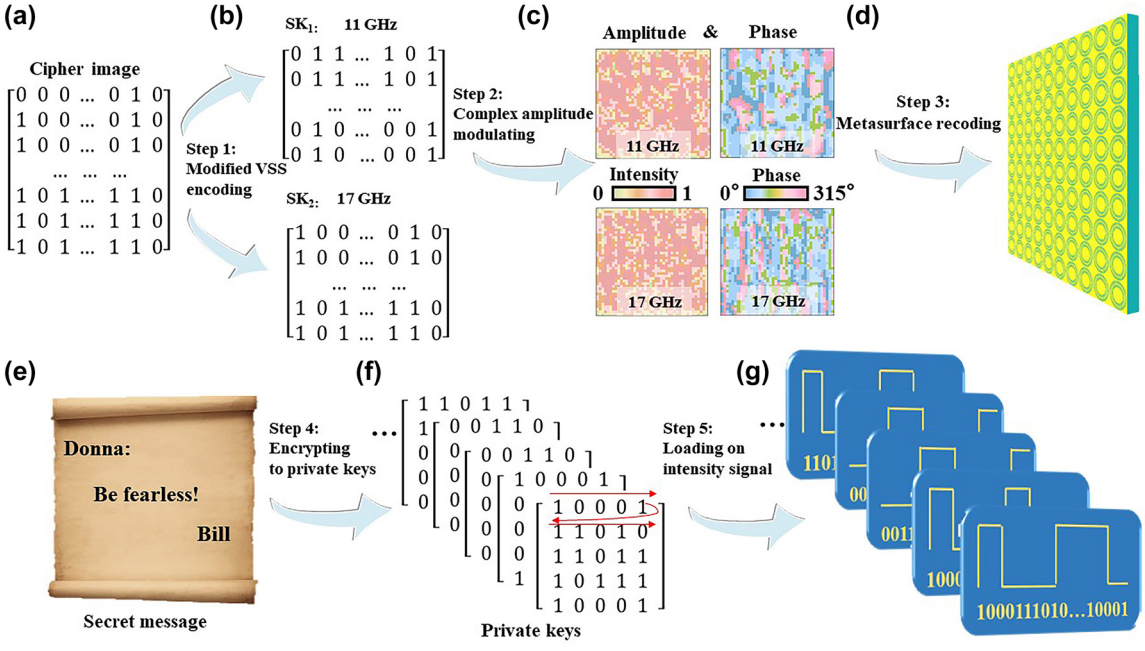

Figure 3: The process of the proposed cryptography method based on the dual-band complex-amplitude metasurface. (a) The cipher image. (b) The shared keys (SKs). (c) The optimized amplitude and phase patterns for the SKs. (d) The dual-band complex-amplitude metasurface. (e) The secret message. (f) The corresponding private keys. (g) The intensity signal loaded private keys.

scheme. Besides, it can be seen from Figure 3(b) that no single SK can be used to disclose the whole secret message, which could enhance the security. Considering the SKs are images composed of white pixel '1' and black pixel '0', as many pixel values as possible should be discretized during the complex-amplitude modulation process to better reconstruct the SKs. The details about the how to design SK_1 and SK_2 could be seen in Section II the supporting information. It is found that the edge characteristics of the SKs can be well reappeared when the pixel corresponds to 3×3 or more units. Following the optimization process, the edge characteristics of the pixel can be well reconstructed by the dual-band metasurface consisting of 42×42 meta-atoms. It is worth mentioning that the results can be further improved by employing a larger metasurface array. In addition, 3-bit phase modulation and six-level amplitude modulation are adopted. Compared to the traditional phase-only encoding method, the complex-amplitude modulation method could improve the quality of the reconstructed holographic SKs to further avoid fidelity loss in the decrypted results [49].

Moreover, the employed private key is also composed of a 5×5 matrix illustrated in Figure 3(f), which is a crucial component of the encryption process. By altering any one of these matrix elements, a new pattern can be produced, resulting in a possible total of 2^{25} unique patterns. Then, the complex-amplitude modulated method is used to hide the SKs into the amplitude and phase distributions displayed in Figure 3(c) by the GS algorithm, which are then recoded into a dual-band metasurface shown in Figure 3(d). Moreover, the transmitter looks up the corresponding private keys according to the secret message (shown in Figure 3(e)) by symbol in the private key dictionary shown in Figure 3(f). Subsequently, the private keys are loaded on the intensity signals to be transmitted shown in Figure 3(g). In this way, a large number of private keys can be transmitted simultaneously in parallel if required. By combining the two frequency-selective SKs, complex-amplitude modulation, and one-time-pad private key, the proposed method could achieve ultra-massive capacity with a much higher-level security and fidelity in comparison to traditional schemes.

2.3 Decryption method

The decryption process can be divided into three steps. First, the two SKs (i.e., the two holographic images) are reconstructed at the pre-set image plane, and the intensity signals as the private keys are received from wireless channel. Next, the SKs are superimposed to form a cipher image by applying an "XNOR" operation. Then, each symbol in the message can be decrypted by performing an "XOR" operation on the cipher image and the private key.

The feasibility of the proposed encoding scheme is firstly verified by numerical calculations and full-wave simulations. Figure 4(a) shows that the numerically calculated SKs can be clearly observed at two pre-set frequencies, which are consistent with the original ones in Figure 3(b). Additionally, a message of "Donna: Be fearless! Bill" is used to demonstrate the capability of the proposed encryption method. The private keys and the corresponding decrypted results for each symbol are depicted in Figure 4(b). The period "·"means the end of the message. If the decrypted results do not contain this symbol, the transmitted message is incomplete and must be retransmitted. Moreover, the key dictionary consisting of private keys and their corresponding decrypted results calculated by MATLAB is shown in Figure S3 in the Supporting Information. Remarkably, different message can be generated by only changing the private keys that are loaded onto the intensity signals, enabling the secret message to be dynamically adjusted from the decryption end.

2.4 Experiment and discussion

In the full-wave simulations, the SKs at two pre-set frequencies could be extracted on the image plane under an RCP plane wave incidence in the CST Microwave Studio. The observation plane is located at a distance of $d = 100$ mm away from the metasurface and parallel to the metasurface. Figure 4(c) plots the two simulated SKs, which are in good agreement with the calculated ones in Figure 4(a). In addition, Figure 4(d) depicts the decrypted results with the provided private keys, which contain 26 letters, 10 numbers, and some special symbols. Noteworthy, this cryptography can theoretically encrypt 2^{25} different patterns, which facilitates the transmission of a greater volume of more intricate information while mitigating potential ambiguities during information dissemination. Some discrepancies between the theoretical calculations and the simulations might be caused by non-ideal edge diffraction of the metasurface in the full-wave simulations and losses in amplitude and phase quantization.

To experimentally validate the proposed method, the designed dual-band metasurface is fabricated and measured. The experimental setup for near-field measurement is illustrated in Figure 5(a). To cover the operating frequencies of 11 and 17 GHz, a pair of dual circularly polarized horn antennas (LB-SJ-60180-P03, 6–18 GHz) was employed as the transmitter and receiver. A quasi-plane wave can be generated by placing a dielectric lens in front of the transmitter, which was then illuminated onto the metasurface sample as

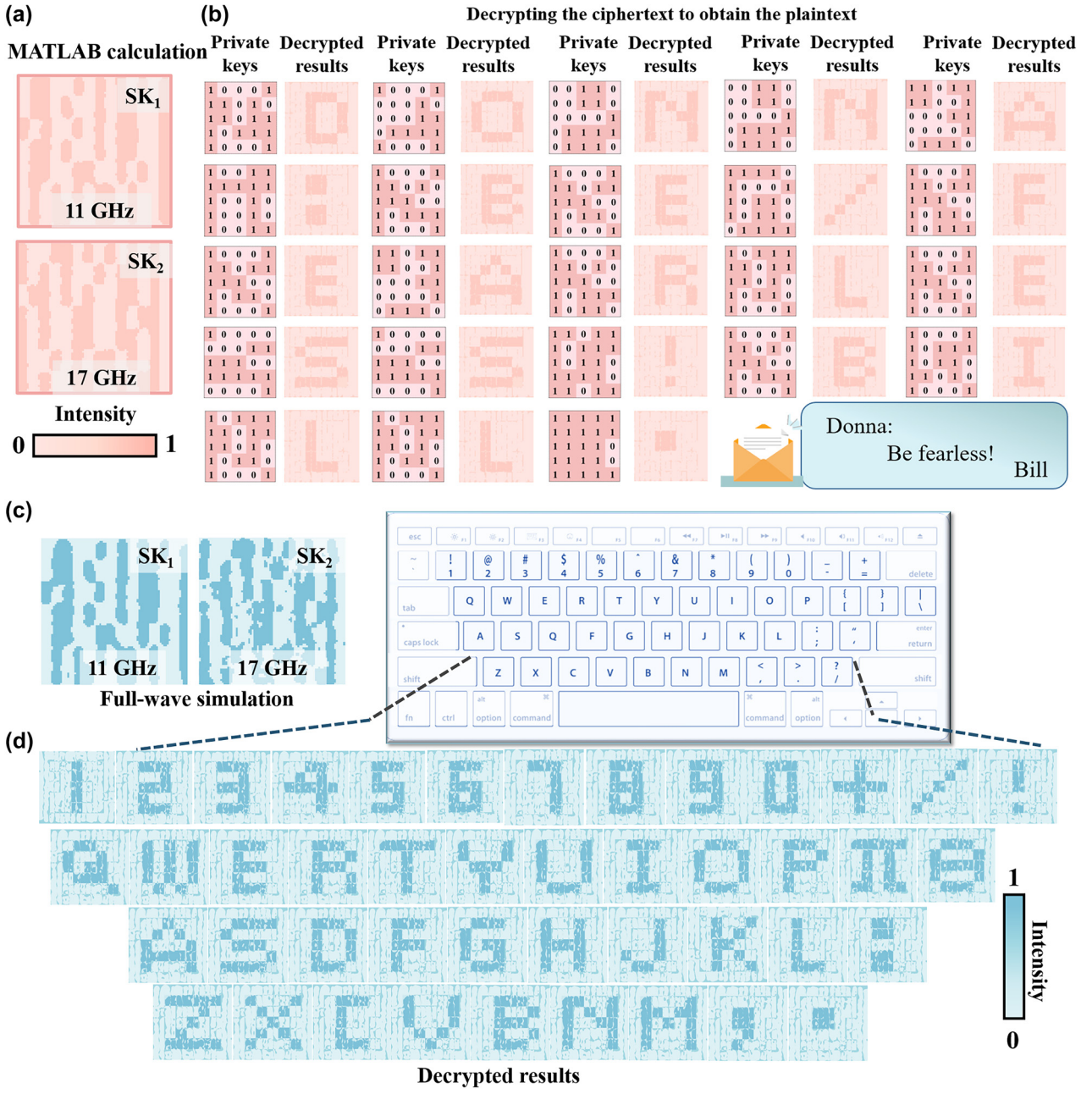

Figure 4: The shared keys (SKs) of MATLAB calculations and full-wave simulations, and their corresponding decrypted results. (a) The SKs calculated by MATLAB. (b) The private key and the corresponding decrypted results (Donna: Be fearless! Bill. "/" represents space, "." indicates the end of the secret message). (c) The full-wave simulations of the SKs, and (d) the corresponding decrypted results.

shown in Figure 5(b). To measure the transmitted fields, the receiver connected to a vector network analyser (Keysight Technologies, N5227B) was moved with a step of 2 mm in both x- and y-directions on the image plane at a distance of $d = 100$ mm from the metasurface. Figure 5(c) shows the metasurface sample composed of 42×42 meta-atoms with an overall dimension of 336 mm $\times$ 336 mm, which was fabricated by the standard printed circuit board (PCB) fabrication process.

Figure 6(a) plots the measured SKs at the two operating frequencies, which are in good consistency with the calculated and simulated ones depicted in Figure 5(a) and (c). The quality of the measured SKs could be impacted by several factors including the fabrication tolerance, losses in amplitude and phase quantization, and the measurement tolerance. It is noteworthy that each shared unit in the reconstructed SKs should have a significant marginalization feature without obvious distortion between adjacent units

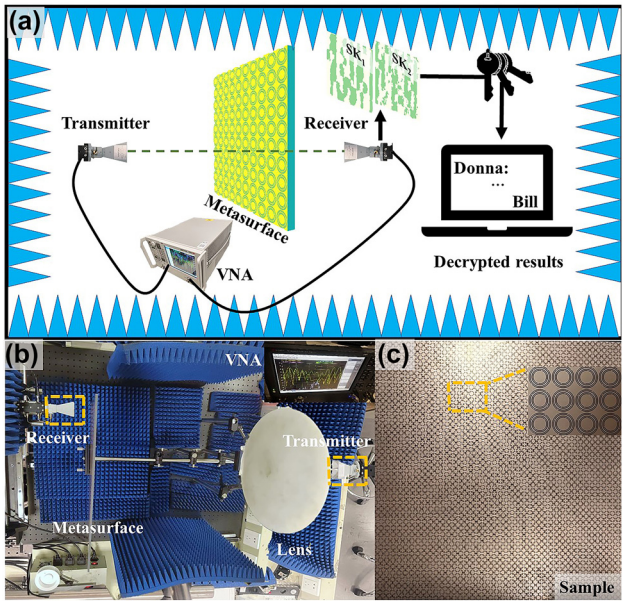

Figure 5: The experimental setup and the fabricated metasurface prototype. (a) The schematic diagram of the experimental setup for decoding the secret message. (b) The photograph of the experimental setup. (c) The fabricated metasurface prototype.

in order to achieve complete decryption of the message. The comparison of the cross sections of the electric fields for two reconstructed SKs obtained by numerical calculation, full-wave simulation, and experimental measurement, are conducted. The normalized electric fields are collected at the cross sections of Figure 6(a) along the pink dashed lines. It is evident from Figure 6(c) and (d) that the SKs with various bit values of 1 and 0 can be identified very well. In the MATLAB calculations, each unit cell is simplified as an ideal dipole with the corresponding phase and amplitude, which could provide a much faster numerical calculation of the meta-hologram compared to the full-wave simulations. Additionally, it is noted that the SKs have well-defined edge details due to the complex-amplitude modulation, which is very helpful for subsequent decryption processes.

Figure 6(b) presents the decrypted results of 10 numbers, 26 letters, and some special symbols obtained by the decryption process. It can be observed from Figure 6(b) that the decrypted results can be well recognized and agree very well with the design objects despite of a little decreased quality. Moreover, Figure 6(e) plots the correlation coefficients (COs) between the decrypted results and the original message, which is used to quantitatively evaluate the decoding quality of the decrypted patterns. Both numerical calculation and full-wave simulation results show higher values, verifying higher decoding qualities of the secret patterns. The COs from experiments are relatively low due to the errors in sample processing and experimental testing. In particular, the ideal plane wave in the simulation is configured to impinge directly on the metasurface, whereas the incident wave from the horn antenna in the measurement is not an ideal plane wave. Even though there are some distortions and noises in the decrypted results, the contrast of these results remains discernible to naked eyes. Overall, the revealed parameters verify the capabilities of the proposed cryptography for encoding ultra-massive distinct patterns and guaranteeing a high fidelity of decrypted results simultaneously.

2.5 Security and capacity analysis

In the field of cryptography, the security and fidelity are of vital importance. Due to the direct holographic imaging used for the decoding process in traditional metasurface-empowered cryptography, there is a risk of information leakage when a single message is encoded into a single channel. To tackle this issue, the VSS scheme is adopted to hide the secret message into multiple SKs, significantly enhancing the security of the cryptography. However, some information of the decryption result cannot be fully recovered in the VSS scheme as shown in Figure S2(b). To overcome this, a modified VSS scheme is used, unlocking new possibilities for the metasurface-empowered cryptography with a higher fidelity. Moreover, the private key is used to promise for a high security cryptography. Even if the eavesdropper obtains the SKs, the secret message cannot be cracked without the private key. Moreover, even when the SKs and private key are known, the secret message cannot be obtained without knowing the superposition logic of the SKs and the private keys, which provides a new avenue for high-security cryptography.

For metasurface-empowered cryptography, the coverage of the content is as important as security. In traditional metasurface-empowered cryptography, the number of secret messages depends on the number of channels of the metasurface. However, due to the nearly exhausted available channels for information multiplexing, it becomes very challenging to send more information. To overcome this restriction, the proposed metasurface-empowered cryptography can encode a total of 2^{25} different patterns by using 25-bit binary string as the private key, greatly increasing the coverage of secret information. Moreover, the 2^{25} patterns are independent of each other since we encoded the private key into sets of intensity signals. Furthermore, we can send various encrypted message using the same metasurface by simply altering the private keys, which is also known as the “one-time-pad” encryption method. Such a strategy breaks the limitation of the

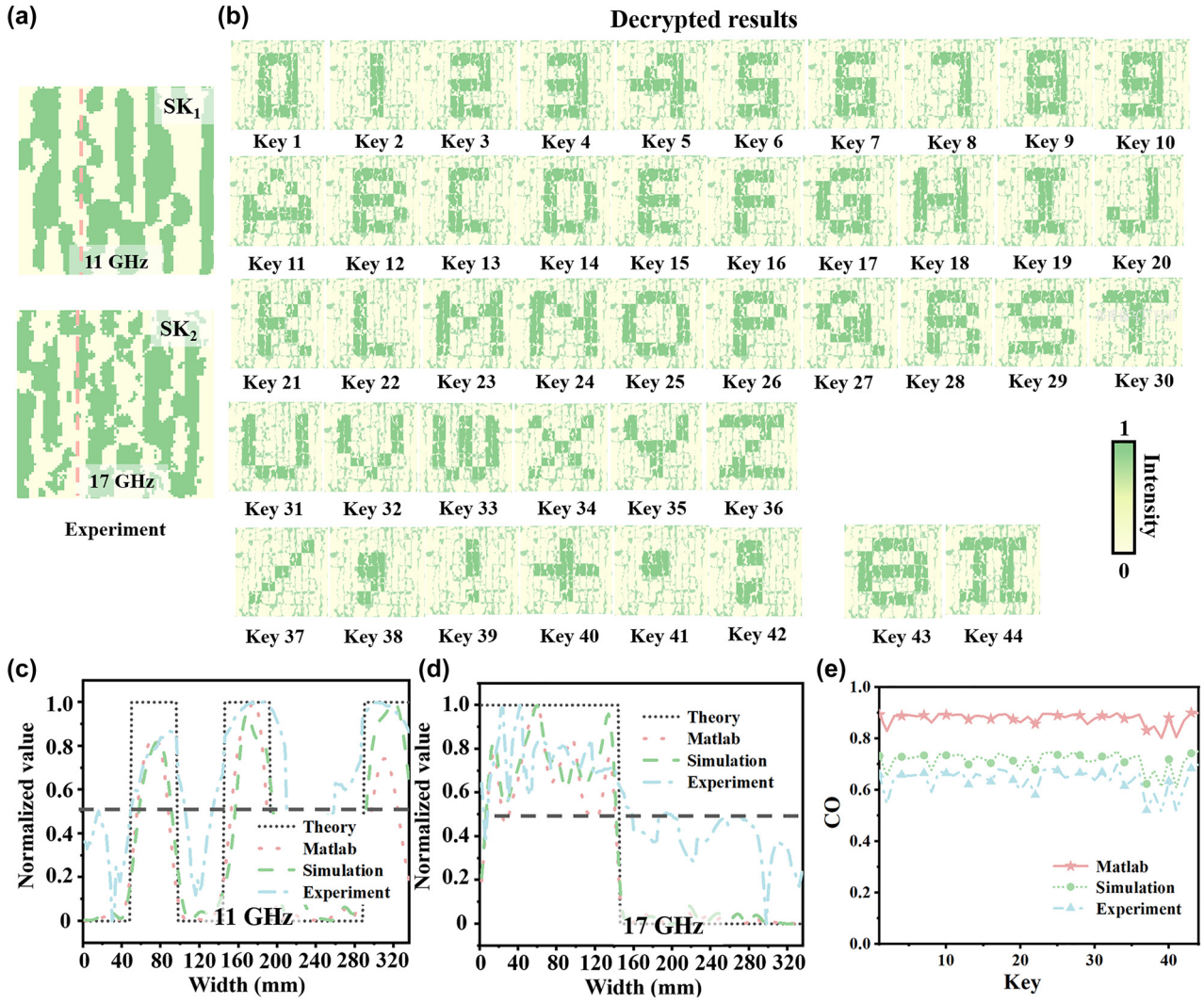

Figure 6: The measured results and the comparisons. The measured results of (a) the SKs and (b) the corresponding decrypted results. The comparison of the (c) SK_1 and (d) SK_2 fields obtained by the diffraction theory, MATLAB calculation, full-wave simulation, and experimental measurement. (e) The correlation coefficients (COs) obtained by the MATLAB calculation, simulation and experiment results of decrypted results under the extraction of 44 different private key sequences.

storage on metasurfaces, providing a novel platform for large-coverage encryption and dynamically adjusting secret message.

3 Conclusion

In summary, we propose a novel cryptography method based on two frequency-selective SKs generated from a complex-amplitude metasurface and the one-time-pad private keys. Firstly, the features of ultra-massive different patterns (a total of 2^{25} in this work) are extracted as a cipher image and converted into the SKs by the modified VSS scheme, which could heighten the fidelity of the decrypted result. Moreover, the two SKs are encoded into the amplitude and phase distributions based on the iterative GS algorithm and recoded into a dual-band meta-hologram with complex-amplitude modulation, aiming to improve the decryption quality. During the decryption phase, two SKs can be reconstructed at two pre-set frequencies under a RCP incidence, and the private key represented by a set of 25-bit intensity signals can be received from wireless channel. Afterwards, the two SKs are superimposed in accordance with the decoding mechanism of the modified VSS scheme to create a cipher image. Each symbol in the secret message can be then decrypted by performing an “XOR” operation on the cipher image and each private key. In this way, the secret message cannot be deciphered by either the SKs or the private keys. To experimentally verify the proposed approach, a meta-hologram was fabricated and measured,

and the measured results demonstrate good agreement with numerical ones and targets. By combining the SKs and different private keys, the proposed metasurface-empowered cryptography can significantly improve the security and the capacity of the secret patterns, offering a new promising route for encryption. Furthermore, by simply changing the private keys or the intensity signal sequences, the transmitted message can be dynamically alternated with the same metasurface.

Research funding: This work was supported by the National Natural Science Foundation of China (Grant nos. 62171186 and 62271056), China Postdoctoral Science Foundation (Grant no. 2023M731827), and the National Key R&D Program of China (Grant no. 2022YFF0604801).

Author contributions: Zhen Gu and Rensheng Xie contributed equally to this work. JD, SC, and HZ conceived the methodology concepts. ZG and RX completed the theoretical model and wrote the manuscript. HL and XW performed the experiments. YL and JG assisted in data collection and processing. JD and LS supervised and coordinated the project. All authors contributed to technical discussions and revise the manuscript regarding this work.

Conflict of interest: Authors state no conflicts of interest.

Data availability: The datasets generated and analysed during the current study are available from the corresponding author upon reasonable request.

References

[1] Q. Wang, B. Lin, M. Chen, C. Zhao, H. Tian, and D.-H. Qu, "A dynamic assembly-induced emissive system for advanced information encryption with time-dependent security," *Nat. Commun.*, vol. 13, no. 1, p. 4185, 2022.

[2] Y. Zhang, *et al*., "DNA origami cryptography for secure communication," *Nat. Commun.*, vol. 10, no. 1, p. 5469, 2019.

[3] J. Yin, *et al*., "Entanglement-based secure quantum cryptography over 1,120 kilometres," *Nature*, vol. 582, no. 7813, pp. 501—505, 2020.

[4] M. Yang, L. Zhu, Q. Zhong, R. E. Ganainy, and P. Y. Chen, "Spectral sensitivity near exceptional points as a resource for hardware encryption," *Nat. Commun.*, vol. 14, no. 1, p. 1145, 2023.

[5] A. C. Boukis, K. Reiter, M. Frölich, D. Hofheinz, and M. A. R. Meier, "Multicomponent reactions provide key molecules for secret communication," *Nat. Commun.*, vol. 9, no. 1, p. 1439, 2018.

[6] D. Wen, J. J. Cadusch, J. Meng, and K. B. Crozier, "Multifunctional dielectric metasurfaces consisting of color holograms encoded into color printed images," *Adv. Funct. Mater.*, vol. 30, no. 3, p. 1906415, 2020.

[7] R. Zhao, *et al*., "Multichannel vectorial holographic display and encryption," *Light Sci. Appl.*, vol. 7, no. 1, p. 95, 2018.

[8] Z. L. Deng, *et al*., "Diatomic metasurface for vectorial holography," *Nano Lett.*, vol. 18, no. 5, pp. 2885—2892, 2018.

[9] Q. Song, *et al*., "Ptychography retrieval of fully polarized holograms from geometric-phase metasurfaces," *Nat. Commun.*, vol. 11, no. 1, p. 2651, 2020.

[10] Y. Hu, *et al*., "All-dielectric metasurfaces for polarization manipulation: principles and emerging applications," *Nanophotonics*, vol. 9, no. 12, pp. 3755—3780, 2020.

[11] F. Ding, S. Tang, and S. I. Bozhevolnyi, "Recent advances in polarization-encoded optical metasurfaces," *Adv. Photonics Res.*, vol. 2, no. 6, p. 2000173, 2021.

[12] C. Kim, Y. Kim, D. Kang, and M. Lee, "Laser-printed emissive metasurface as an anticounterfeiting platform," *Laser Photonics Rev.*, vol. 16, no. 10, p. 2200215, 2022.

[13] G. Qu, *et al*., "Reprogrammable meta-hologram for optical encryption," *Nat. Commun.*, vol. 11, no. 1, p. 5484, 2020.

[14] S. M. Kamali, E. Arbabi, A. Arbabi, Y. Horie, M. Faraji-Dana, and A. Faraon, "Angle-multiplexed metasurfaces: encoding independent wavefronts in a single metasurface under different illumination angles," *Phys. Rev.*, vol. 7, no. 4, p. 041056, 2017.

[15] S. S. Kruk, *et al*., "Asymmetric parametric generation of images with nonlinear dielectric metasurfaces," *Nat. Photonics*, vol. 16, no. 8, pp. 561—565, 2022.

[16] Y. Chen, X. Yang, and J. Gao, "3D Janus plasmonic helical nanoapertures for polarization-encrypted data storage," *Light Sci. Appl.*, vol. 8, no. 1, p. 45, 2019.

[17] H. Ren, *et al*., "Metasurface orbital angular momentum holography," *Nat. Commun.*, vol. 10, no. 1, p. 2986, 2019.

[18] Y. Shen, *et al*., "Optical vortices 30 years on: OAM manipulation from topological charge to multiple singularities," *Light Sci. Appl.*, vol. 8, no. 1, p. 90, 2019.

[19] X. Fang, H. Ren, and M. Gu, "Orbital angular momentum holography for high-security encryption," *Nat. Photonics*, vol. 14, no. 2, pp. 102—108, 2020.

[20] X. Luo, *et al*., "Integrated metasurfaces with microprints and helicity-multiplexed holograms for real-time optical encryption," *Adv. Opt. Mater.*, vol. 8, no. 8, p. 1902020, 2020.

[21] H. Zhou, *et al*., "Polarization-encrypted orbital angular momentum multiplexed metasurface holography," *ACS Nano*, vol. 14, no. 5, pp. 5553—5559, 2020.

[22] Z. Deng, *et al*., "Full-color complex-amplitude vectorial holograms based on multi-freedom metasurfaces," *Adv. Funct. Mater.*, vol. 30, no. 21, p. 1910610, 2020.

[23] D. Wen, J. J. Cadusch, J. Meng, and K. B. Crozier, "Light field on a chip: metasurface-based multicolor holograms," *Adv. Photonics*, vol. 3, no. 02, p. 024001, 2021.

[24] M. Song, *et al*., "Enabling optical steganography, data storage, and encryption with plasmonic colors," *Laser Photonics Rev.*, vol. 15, no. 3, p. 2000343, 2021.

[25] R. Feng, *et al*., "A modular design of continuously tunable full color plasmonic pixels with broken rotational symmetry," *Adv. Funct. Mater.*, vol. 32, no. 7, p. 2108437, 2022.

[26] J. Kim, *et al*., "Photonic encryption platform via dual-band vectorial metaholograms in the ultraviolet and visible," *ACS Nano*, vol. 16, no. 3, pp. 3546—3553, 2022.

[27] Y. Bao, *et al*., "Coherent pixel design of metasurfaces for multidimensional optical control of multiple printing-image switching and encoding," *Adv. Funct. Mater.*, vol. 28, no. 51, p. 1805306, 2018.

[28] H. Zhou, *et al*., "Correlated triple hybrid amplitude and phase holographic encryption based on a metasurface," *Photonics Res.*, vol. 10, no. 3, p. 678, 2022.
[29] X. Zang, *et al*., "Polarization encoded color image embedded in a dielectric metasurface," *Adv. Mater.*, vol. 30, no. 21, p. 1707499, 2018.
[30] X. Guo, *et al*., "Full-color holographic display and encryption with full-polarization degree of freedom," *Adv. Mater.*, vol. 34, no. 3, p. 2103192, 2022.
[31] L. Jin, *et al*., "Noninterleaved metasurface for (2^6 -1) spin-and wavelength-encoded holograms," *Nano Lett.*, vol. 18, no. 12, pp. 8016—8024, 2018.
[32] X. Fang, *et al*., "High-dimensional orbital angular momentum multiplexing nonlinear holography," *Adv. Photonics*, vol. 3, no. 1, p. 015001, 2021.
[33] J. Yan, *et al*., "Single pixel imaging key for holographic encryption based on spatial multiplexing metasurface," *Small*, vol. 18, no. 35, p. 2203197, 2022.
[34] Z. Li, *et al*., "Polarization-assisted visual secret sharing encryption in metasurface hologram," *Adv. Photonics Res.*, vol. 2, no. 11, p. 2100175, 2021.
[35] Z. Li, *et al*., "Cryptography metasurface for one-time-pad encryption and massive data storage," *Laser Photonics Rev.*, vol. 16, no. 8, p. 2200113, 2022.
[36] Z. Li, M. Premaratne, and W. Zhu, "Advanced encryption method realized by secret shared phase encoding scheme using a multi-wavelength metasurface," *Nanophotonics*, vol. 9, no. 11, pp. 3687—3696, 2020.
[37] C. Shen, J. Sun, Y. Qi, S. Lv, and S. Wei, "Electrically tunable all-dielectric metasurfaces integrated with nematic liquid crystals for information encryption," *IEEE Photonics J.*, vol. 13, no. 4, pp. 1—5, 2021.
[38] Q. Xiao, *et al*., "Orbital-angular-momentum-encrypted holography based on coding information metasurface," *Adv. Opt. Mater.*, vol. 9, no. 11, p. 2002155, 2021.
[39] F. Walter, G. Li, C. Meier, S. Zhang, and T. Zentgraf, "Ultrathin nonlinear metasurface for optical image encoding," *Nano Lett.*, vol. 17, no. 5, pp. 3171—3175, 2017.
[40] D. Hu, *et al*., "Laser-splashed three-dimensional plasmonic nanovolcanoes for steganography in angular anisotropy," *ACS Nano*, vol. 12, no. 9, pp. 9233—9239, 2018.
[41] H. Ren, X. Fang, J. Jang, J. Bürger, J. Rho, and S. A. Maier, "Complex-amplitude metasurface-based orbital angular momentum holography in momentum space," *Nat. Nanotechnol.*, vol. 15, no. 11, pp. 948—955, 2020.
[42] J. Deng, *et al*., "Metasurface-assisted optical encryption carrying camouflaged information," *Adv. Opt. Mater.*, vol. 10, no. 16, p. 2200949, 2022.
[43] J. Li, S. Kamin, G. Zheng, F. Neubrech, S. Zhang, and N. Liu, "Addressable metasurfaces for dynamic holography and optical information encryption," *Sci. Adv.*, vol. 4, no. 6, p. 6768, 2018.
[44] H. Zhou, *et al*., "Switchable active phase modulation and holography encryption based on hybrid metasurfaces," *Nanophotonics*, vol. 9, no. 4, pp. 905—912, 2020.
[45] M. Ouyang, *et al*., "Optical encryption in spatial frequencies of light fields with metasurfaces," *Optica*, vol. 9, no. 9, p. 1022, 2022.
[46] J. Deng, *et al*., "Multiplexed anticounterfeiting meta-image displays with single-sized nanostructures," *Nano Lett.*, vol. 20, no. 3, pp. 1830—1838, 2020.
[47] Y. Wang, *et al*., "Extreme diffraction management in phase-corrected gradient metasurface by fourier harmonic component engineering," *Laser Photonics Rev.*, vol. 17, no. 7, p. 2300152, 2023.
[48] K. Zhang, Y. Wang, S. N. Burokur, and Q. Wu, "Generating dual-polarized vortex beam by detour phase: from phase gradient metasurfaces to metagratings," *IEEE Trans. Microwave Theory Tech.*, vol. 70, no. 1, pp. 200—209, 2023.
[49] R. Xie, *et al*., "Frequency-multiplexed complex-amplitude meta-devices based on bispectral 2-bit coding meta-atoms," *Adv. Opt. Mater.*, vol. 8, no. 24, p. 2000919, 2020.

Supplementary Material: This article contains supplementary material (https://doi.org/10.1515/nanoph-2024-0314).