ACS APPLIED MATERIALS & INTERFACES

www.acsami.org

Research Article

High-Security Data Encryption Enabled by DNA Multi-Strand Solid-Phase Hybridization and Displacement in Inkjet-Printed Microarrays

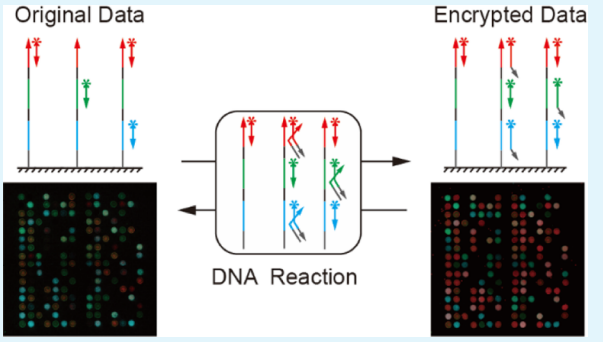
Ben Pei, Jiaxiang Ma, Liliang Ouyang, and Zhuo Xiong*

Cite This: *ACS Appl. Mater. Interfaces* 2025, 17, 10179−10190

Read Online

ACCESS | Metrics & More | Article Recommendations | Supporting Information

ABSTRACT: Multicolor fluorescent encryption systems that respond to specific stimuli have drawn widespread attention to data storage and encryption due to their low cost and facile data access. However, existing encryption systems are limited by encryption materials, restricting their encryption depth. This study uses DNA molecules as encryption materials that offer exceptional specificity and encryption depth within sequences. With inkjet-printed microarrays on a solid-phase interface, a multicolor fluorescent data storage system based on DNA hybridization and strand displacement is developed, achieving an encryption system with high encryption depth and flexibility. DNA strands, modified with different fluorescent labels, are delivered onto solid-phase interfaces containing a DNA self-assembled monolayer (SAM) via inkjet printing, forming multicolor fluorescent data microarrays. Data storage and encryption are achieved through the hybridization of fluorescent DNA strands for data presentation and interference with the DNA SAM at the interface between the solid phase and droplets. Interference DNA strands can be removed by DNA strand displacement for decryption. The encryption depth of this system is determined by the design of the DNA sequences and the combination of multiple DNA strands, showcasing its outstanding encryption ability. Meanwhile, high-throughput inkjet printing accelerates the data writing process, further enhancing the system efficiency. With DNA solid-phase reaction in inkjet-printed microarrays, this system provides a scalable and robust strategy for high-depth and efficient data encryption.



KEYWORDS: *data encryption, inkjet printing, solid-phase DNA hybridization, DNA strand displacement, DNA nanotechnology*

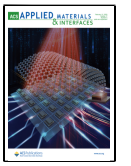
1. INTRODUCTION

With the rapid development of data technology, ensuring the data security has become a critical challenge, particularly in sectors such as finance.[1−3] To meet this demand, research has increasingly focused on anticounterfeiting methods, optical encryption systems, and molecular data coding strategies, offering innovative methods to enhance data security and integrity.[4−6] Among these approaches, optical encryption leveraging colorimetric changes has emerged as a particular solution due to its inherent versatility and notable advancements.[1,7−10] This is largely attributed to the unique properties of encryption materials, which can undergo specific color transitions in response to external stimuli. These attributes, coupled with their cost-effectiveness and rapid response times, make them ideal for practical applications.[11−13]

Encryption systems based on controlled optical color changes under specific stimuli have shown diverse advancements in recent years.[14−17] For example, Otaegui et al. developed thermoresponsive fluorescent materials by combining fluorescent groups with organic phase-change materials, resulting in multicolor microcapsules for Encryption.[18] These materials were used to construct data arrays that exhibited distinct colorimetric patterns at specific temperatures, enabling encrypted data storage. Similarly, Li et al. employed humidity-responsive polymers to print total internal reflection structural color arrays, creating an encryption system controlled by relative humidity.[19] These studies, which rely on specific stimuli for data encryption, demonstrate great potential. Utilizing stimuli factors such as temperature,[14,18] relative humidity,[19−21] pH levels,[22,23] ambient oxygen concentrations,[24] and light inputs[25−27] allows these systems to selectively switch between encrypted states and decrypted states, ensuring robust data security.

A variety of encryption methods have been developed to demonstrate effective data security. However, many of these approaches rely on specific external stimuli, limiting their encryption depth. This constraint makes them vulnerable to decryption attempts. DNA molecules, as a promising material with extraordinary potential in high-density data storage, allow

Received: December 10, 2024
Revised: January 22, 2025
Accepted: January 23, 2025
Published: January 29, 2025



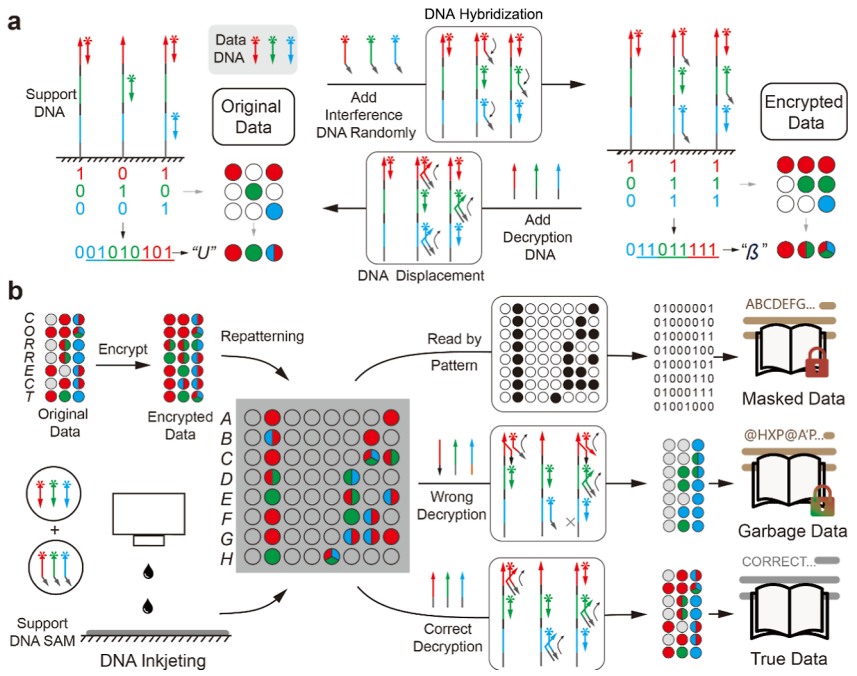


Figure 1. Mechanism and process of data encryption. (a) Mechanism of data storage and encryption. Fluorescent data DNA strands are hybridized onto three spots with the support DNA, where the fluorescence combination forms "001010101" to encode the original data "U". Fluorescent interference DNA strands are randomly added to available sequences on the support DNA, altering the fluorescence combination to "011011111" for data encryption to "β". By adding decryption DNA and performing DNA strand displacement, the interference DNA can be removed, enabling data decryption. (b) Data encryption and decryption process. The original data "CORRECT" is encoded into multicolor fluorescent combination spots and encrypted. The fluorescence data spots are rearranged to form the pattern encoding the masked data "ABCDEFGH" through inkjet printing of data and interference DNA. When this pattern is read, only the masked data are obtained. When wrong decryption DNA is added, reading the fluorescence combination spots results in garbage data. Only the correct decryption DNA can remove the interference DNA correctly, allowing the true data to be retrieved.

for encoding large amounts of data in limited space.[28−32] As functional biomolecules, DNA molecules can realize hybridization, strand displacement, and origami with high specificity, offering a wider range of encryption options with enhanced encryption depth.[33−36] DNA molecules can also be chemically modified with incorporated fluorescent labels. This allows their complex sequence data to be easily detected and characterized through fluorescence.[37] Furthermore, DNA systems can realize more complex computations like logic gate and even neural network, with fluorescence signals reflecting the outcomes.[38−42] However, there is a notable lack of effective multibit fluorescence encryption systems based on coupled DNA strand displacement. This is due to conflicts among several critical requirements. These include the demand for small space to achieve high storage density, the complexity of pattern formation needed for multibit fluorescence arrays, and the multicomponent reactions necessary for coupled DNA hybridization and strand displacement in solid-phase systems.

In this work, we propose a novel multicolor fluorescence storage system based on inkjet-printed microarrays to address the challenges. This low-cost and highly efficient method uses single-stranded DNA self-assembled into a monolayer as the substrate. Fluorescently labeled DNA strands are deposited via inkjet printing to specific locations, where they hybridize with the substrate DNA to form fluorescent arrays for data storage. Special interference strands, indistinguishable from the data strands due to their identical fluorescence, are also introduced to the array. These strands couple with the data strands and can be selectively removed by specific decryption strands via DNA strand displacement, enabling robust encryption and decryption. This system supports the design of diverse DNA sequences for advanced encryption and enables a complex strand displacement logic. By integrating sequence diversity and multistrand combination, it achieves exceptionally high encryption depth.

The DNA droplets formed by inkjet printing are in the picoliter range, enabling microdots as small as tens of micrometers. This ensures a high data storage density while minimizing resource consumption. Inkjet printing can also deposit multiple DNA inks parallelly, allowing for the creation of complex patterns in a short time. This process enables data writing in one step through simultaneous printing and hybridization. Overall, this system employs DNA molecules with fluorescence as materials for data storage and encryption and uses inkjet printing to achieve a low-cost, efficient, and scalable solid-phase microarray reaction platform. By combination of these elements, this system offers a practical and innovative approach, providing new insights into the application of DNA molecules and advanced encryption techniques.

2. EXPERIMENTAL SECTION

2.1. Materials and Reagents. Carboxyl-modified slides were purchased from Xi'an Qiyue Biotechnology. *N*-Hydroxysuccinimide (NHS) was obtained from Amethyst, and 1-ethyl-3-(3-(dimethylamino)propyl)carbodiimide (EDC) from J&K Scientific. 2-Morpholino-ethanesulfonic acid (MES) was sourced from Macklin Reagents. Phosphate Buffered Saline (PBS) buffer was obtained from Thermo Fisher Scientific. Saline sodium citrate (SSC) buffer and sodium dodecyl sulfate (SDS) were obtained from Boer. All oligonucleotides were synthesized by Sangon Biotech, with their

https://doi.org/10.1021/acsami.4c21723
ACS Appl. Mater. Interfaces 2025, 17, 10179−10190

sequences listed in Supporting Information, Table S1. The buffer used for DNA hybridization and strand displacement consisted of 50 mM NaCl and 5% glycerol dissolved in 1 × TE buffer (10 mM Tris, 0.1 mM EDTA, pH 7.5) from Solabio Bio. Fluorescence imaging was performed using an Olympus confocal fluorescence microscope, with Texas Red, FAM, and Pacific Blue dyes used for red, green, and blue fluorescence, observed at 594, 488, and 405 nm, respectively. The inkjet printer used is from Aure Technology, model BP4000. The nozzle diameter is 22 μm, the driving waveform used is a square wave, and the maximum firing frequency is 12 kHz.

2.2. Printing Substrate Preparation. Dissolve NHS was dissolved at a concentration of 100 mM and EDC at 50 mM in 200 mM MES buffer (pH 6.0) to prepare the activation solution. The carboxyl-modified slides were immersed in the activation solution for 20 min, then rinsed thoroughly with water to remove residual reagents. Amino-modified DNA molecules were prepared by dissolving them in 1× PBS buffer at a final concentration of 2 μM. Using chambers, the DNA solution was loaded onto the activated slides and incubated at 37 °C for 2 h to immobilize the DNA support strands on the slides. After immobilization, the slides were rinsed with 1× PBS buffer and water for 5 min each and then dried with nitrogen gas.

2.3. Inkjet Printing and DNA Hybridization. Glass slides immobilized with support DNA strands serve as the printing substrate. Data DNA strands or interference DNA strands were prepared at a concentration of 10 μM by dissolving them in a hybridization buffer. This DNA solution was loaded into the ink reservoir of the inkjet printer. The DNA solution was printed onto the prepared substrate following a predesigned pattern. To ensure uniform humidity across the printed area, the main pattern was surrounded with additional concentric rings of printed droplets. Postprinting, the slide was placed in a humidified chamber and hybridization allowed to proceed for 1 h at 37 °C. After hybridization, unbound DNA strands were removed by washing the slides sequentially with cleaning buffers: 1× SSC with 0.03% SDS for 5 min, followed by 0.2× SSC for 5 min, and 0.05× SSC for another 5 min. Finally, the slides were rinsed with water and dried using nitrogen gas.

2.4. Solid-Phase DNA Strand Displacement Reaction. To perform the solid-phase DNA strand displacement reaction, 5 μM decryption DNA strand was dissolved in hybridization buffer to create the strand displacement solution. This solution was applied onto the glass slide, which was already hybridized with the data DNA strand, using a pipet. The slide was incubated for 1 h at room temperature in a humid box to allow the strand displacement reaction to take place. Once the reaction was complete, the slide was cleaned with washing buffers: first wash with 1× SSC and 0.03% SDS for 5 min, followed by 0.2× SSC for 5 min, and 0.05× SSC for another 5 min. Finally, the slide was rinsed with ultrapure water and dried with nitrogen gas.

2.5. Image Processing and Data Analysis. Fluorescence images were processed and analyzed using ImageJ. Data analysis was performed using Origin, and the statistical result graphs were generated accordingly.

3. RESULTS AND DISCUSSION

3.1. Mechanism and Design of the System. This system realizes data storage and encryption through DNA solid-phase hybridization and strand displacement. The system uses DNA strands immobilized on a substrate (support DNA) as the template strands, onto which various fluorescently labeled DNA strands for data presentation (data DNA) are hybridized, forming multicolor fluorescent spots for data storage. As shown in Figure 1a, the support DNA sequence is organized from 5′ to 3′as follows: support sequence (gray), hybridization sequence 1 (blue), spacer sequence (black), hybridization sequence 2 (green), spacer sequence (black), and hybridization sequence 3 (red), totaling 66 nucleotides (Figure S1a). The three hybridization sequences are complementary to the corresponding DNA strands, which are labeled with blue, green, and red fluorescence. These data DNA strands hybridize at their specific sites on the support DNA, forming fluorescent spots where fluorescence indicates "1" and no fluorescence indicates "0" for data storage. For example, in three consecutive DNA spots, the first spot hybridizes only with red fluorescence, the second spot hybridizes only with green fluorescence, and the third spot hybridizes with both red and blue fluorescence. The corresponding blue, green, and red fluorescence data are "0 0 1", "0 1 0", and "1 0 1". The fluorescence combination of these three spots forms a 9 bit binary code "001010101" The last 8 bits of this code correspond to the ASCII code for the letter "U". Thus, this system uses the combination of multicolor fluorescence to store the letter "U". Similarly, to encrypt data, DNA strands for data interference (interference DNA) are added randomly at available sequences on the support DNA to obscure the original data. For example, if interference DNA with red and blue fluorescence is added at the second spot and green interference DNA is added at the third spot, the encrypted code becomes "011011111", encrypting "U" to "β". These interference DNA strands contain specific toe sequences that enable their selective removal via DNA strand displacement. Corresponding DNA strands for data decryption (decryption DNA) hybridize with the interference DNA strands and facilitate their removal through strand displacement. Once the interference DNA is displaced and cleared, the original data are decrypted.

Based on this fundamental principle, DNA molecules can be used as encryption materials for various forms of data encryption. This study combines commonly used data masking techniques in data encryption, utilizing inkjet printing to arrange fluorescent data spots into specific patterns and thereby mask them into a particular message. As shown in Figure 1b, a typical example begins with the original message "CORRECT", which is first encoded into a combination of multicolor fluorescence, and then encrypted by encoding interference fluorescence. To achieve the data masking, the fluorescent spots are arranged into a specific pattern, in which fluorescent spots represent "1" and nonfluorescent spots represent "0". The pattern is designed according to the ASCII code for the masked data "ABCDEFGH". Subsequently, using data DNA and interference DNA as the inks and a DNA self-assembled monolayer (SAM) as the substrate, the designed pattern is printed via inkjet technology. If an attacker illuminates the spots to reveal the fluorescence pattern, the masked data are accessed to confuse the attacker, preventing a further decryption attempt. Furthermore, even if the attacker is familiar with the DNA encryption method, they will be unable to decrypt the data without the correct decryption DNA. If they attempt to use various DNA strands for brute-force decryption, the incorrect strands will fail to perform the correct strand displacement reaction, thus unable to remove the interference DNA. As shown in the "wrong decryption" example in Figure 1b, three possible scenarios may occur when attempting brute-force decryption using DNA strands. In most cases, as in the blue attempt strand, the incorrect strand cannot react with the interference strand and will have no effect on the fluorescence. In a rare case, the green attempt strand may accidentally match the correct green decryption DNA, allowing the removal of the green interference DNA. However, as there are three types of interference DNA, the removal of only the green interference DNA will not result in correct decryption.

https://doi.org/10.1021/acsami.4c21723
ACS Appl. Mater. Interfaces 2025, 17, 10179−10190

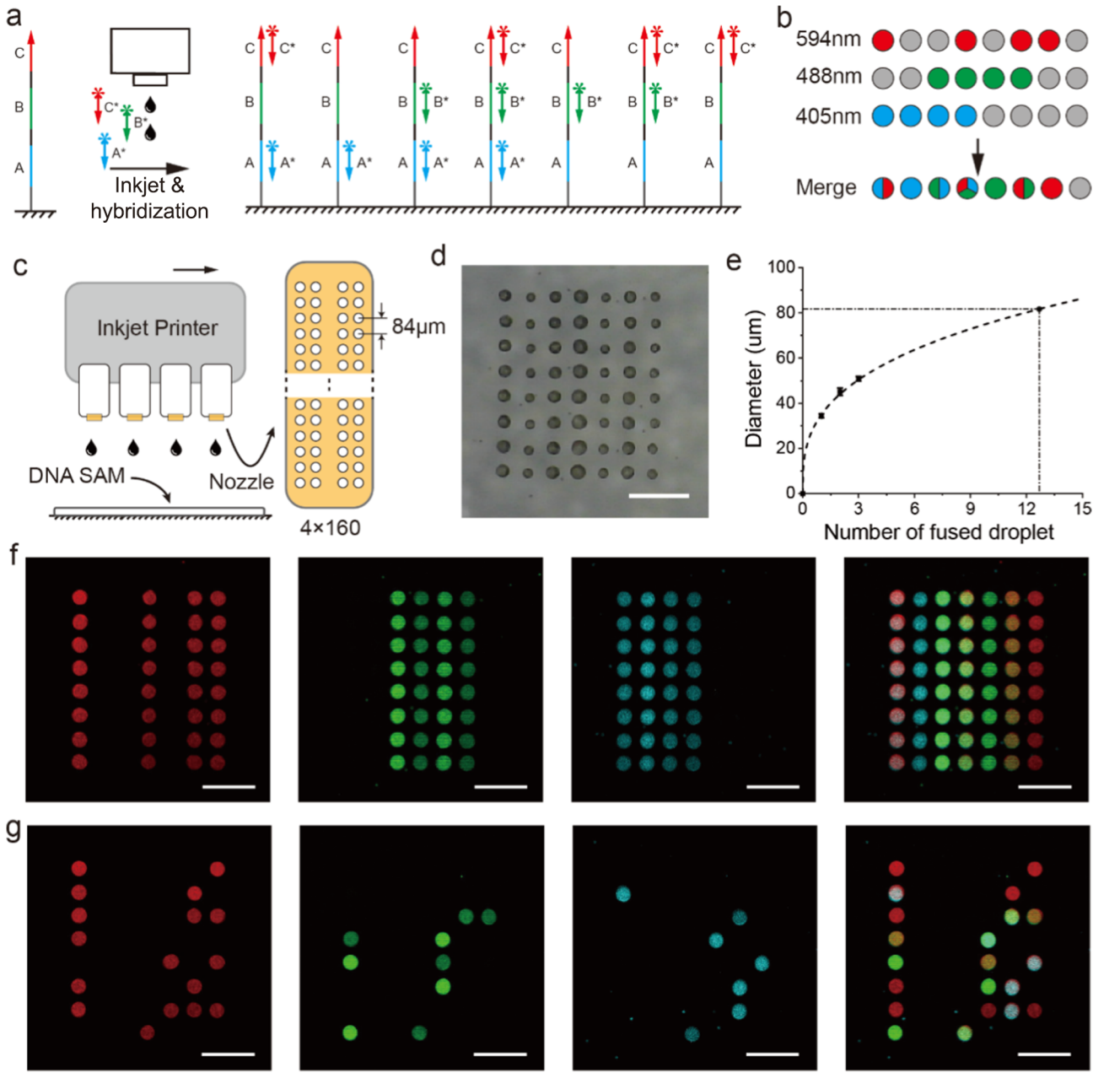


Figure 2. Principle and demonstration of inkjet-printed multicolor fluorescent dot array for DNA hybridization-based data storage. (a) Multi-DNA printing and hybridization test design. (b) Multicolor fluorescence reading design. (c) Schematic illustration of the inkjet printing process. (d) Results of DNA microdroplet printing and droplet fusion (scale bar: 200 μm). (e) The number of fused droplets is proportional to the cube of the droplet radius (n = 8). (f) Fluorescence results of multicolor printing tests (scale bar: 200 μm). (g) Fluorescence results of a sample data test print (scale bar: 200 μm).

Additionally, an attempt strand such as the red attempt strand may cause data corruption, as it will displace the data DNA during strand displacement, thereby damaging the original data and making it irrecoverable. Since the fluorescence of the interference DNA is identical to that of the data DNA, and the addition of interference DNA is random, the attacker cannot identify the interference spots and can attempt decryption only by adding DNA strands for strand displacement. In this article, the decryption DNA strands used are approximately 20 nucleotides in length, and all 60+ bases from the three DNA strands must be correct for successful decryption, providing a very high level of encryption depth. Given the high time and economic costs of DNA synthesis and the potential for damaging the original data during decryption attempts, this system is virtually unbreakable.

3.2. Multicolor Fluorescent Dot Array Data Storage via Inkjet Printing and DNA Hybridization. This study introduces a data storage system based on multicolor dot arrays created by inkjet printing of DNA strands labeled with different fluorescent dyes. The data strands are immobilized onto the substrate of the support DNA SAM via DNA hybridization, enabling efficient data storage. The demonstration of data storage through hybridization and the construction of masked data by forming specific patterns through inkjet printing is shown in Figure 2. The support DNA strand consists of three hybridization regions (A, B, and C),

https://doi.org/10.1021/acsami.4c21723
ACS Appl. Mater. Interfaces 2025, 17, 10179−10190

which are connected by 6 nt spacer regions to prevent unnecessary hybridization interference and provide reaction sites for DNA strand displacement. The substrate used is a glass slide functionalized with carboxyl groups. Through EDC/NHS coupling chemistry, amino-modified support DNA strands are covalently attached to the substrate, forming a DNA SAM interface (Figure S1). Since the DNA hybridization process occurs at the solid−liquid interface, a 6-carbon and 14-thymine nucleotide spacer is included between the amino group and the reaction regions to ensure that the reaction sites are sufficiently distant from the solid-phase interface. To demonstrate the effectiveness of DNA printing and hybridization, data DNA strands (A*, B*, C*) that are complementary to the three hybridization regions of the support DNA strand are used (Figure 2a). All possible combinations of the three data DNA strands are tested to verify the correct hybridization of multiple DNA strands onto the support DNA. Under excitation at 594, 488, and 405 nm, the multicolor fluorescence dots formed by printing and hybridization can be observed (Figures 2b and S2).

This study demonstrates precise DNA delivery to target locations via inkjet printing, ensuring successful fusion of multicomponent DNA droplets and enabling hybridization of multiple DNA strands within a single solid-phase microreaction pool. The inkjet printing head contains 4 × 160 nozzles, enabling highly parallel printing and ensuring high efficiency (Figure 2c). The spacing between the DNA dots is controlled by the spacing between the nozzles, which is 84 μm. Inkjet printing uses solutions of each data DNA as different inks. Through multiink printing, various data DNA strands are deposited onto specific spots on the substrate. Depending on the design, each spot may contain multiple DNA microdroplets that merge into a larger droplet. The droplet size varies depending on the number of fused DNA microdroplets, increasing from 34 μm for single microdroplets to 50 μm for three-microdroplet fusion (Figure 2d). Statistical analysis showed that under the current experimental conditions, a spacing of 84 μm allows for fusion of at least 13 different DNA microdroplets, demonstrating a high limit for multicomponent DNA combination (Figure 2e, Supporting Information Note 1). This limit can be further increased with optimized inkjet printing precision. The composition of the buffer solution is adjusted to ensure stability of the printed droplets in room temperature and humidity environments, effectively preventing evaporation that could impact the fusion and hybridization reactions of multiple DNA microdroplets. In this system, to prevent uneven droplet sizes and DNA concentrations due to the varying number of DNA microdroplets, buffer solution microdroplets are then printed on spots with fewer microdroplets, ensuring uniformity across all spots (Figure S3). Multiple DNA strands simultaneously hybridize with support DNA in micrometer-sized droplets, enabling the construction of complex DNA coupling systems. Thus, the data writing process only requires one printing-hybridization cycle, ensuring the efficiency of the system. After hybridization, DNA strands that fail to hybridize are removed by washing with a buffer solution.

The results of multicolor fluorescence printing and hybridization are shown in Figure 2f. The experimental results indicated that the fluorescence spots formed by inkjet printing had uniform sizes, and various fluorescent DNAs were successfully immobilized onto the substrate through hybridization. Furthermore, specific patterns were formed by inkjet printing to construct the masked data "ABCDEFG" (Figure 2g). The experiment results demonstrated that multicomponent DNA molecules successfully achieved hybridization within the microdroplets, confirming the effectiveness of the inkjet-printed microdroplet solid-phase DNA hybridization system proposed in this study.

Inkjet printing technology, as a high-precision droplet-on-demand technology, facilitates the construction of complex patterns and has been widely applied in the fields of data storage and encryption.[24,43,44] Moreover, inkjet printing can efficiently deliver multiple materials with advantages such as high parallel throughput and low ink consumption, making it extensively used in DNA synthesis, microarray construction, chip analysis, and other fields.[45−48] With these advantages, this study creatively proposes a solid-phase multiple DNA hybridization system that forms a storage system with excellent encryption performance. Previously, Song et al. introduced a DNA multibit nonvolatile memory based on an addressable electrode array and implemented shifting operations through strand displacement.[37] By improving the hybridization speeds through electric fields, they achieved significant breakthroughs. In contrast, the inkjet printing system proposed in this study has more advantages in constructing more complex multibit storage and encryption systems. For constructing multiple DNA strand hybridizations at massive reaction points, inkjet printing allows the simultaneous printing of different DNA strands and can deliver various inks on demand in a single print process. Furthermore, the droplets formed by inkjet printing are on the picoliter scale,[49,50] significantly reducing DNA ink consumption and lowering the cost of encryption storage. These advantages ensure that the proposed storage and encryption system is efficient, low-cost, and highly scalable for more complex applications.

The storage speed depends on the inkjet printing speed and hybridization rate. Since hybridization at multiple sites occurs simultaneously, the time required is independent of the amount of stored data. Therefore, when storing large amounts of data, the printing speed can be used as a reference for the encryption speed. The inkjet printer allows 4 × 160 nozzles to print simultaneously, with a maximum of 12,000 prints per second. Considering the efficiency reduction caused by line breaks, the theoretical storage speed can exceed 400 KB/s. Regarding storage density, the distance d between adjacent sites is 84 μm, and each site has three different fluorescence colors. Considering the redundancy of 0.5 introduced by data masking, the storage density D is calculated as $D = 0.5 \times 3/d^2 = 212.6$ bit·mm^{-2}. Compared to existing fluorescence-based DNA solid-phase strand displacement encryption storage methods,[34] the storage density has increased by 6000 times. Since this system stores data through fluorescent microdots, its storage density is still lower than encryption methods based on DNA sequences[51] and DNA nanostructures.[52] However, compared to DNA sequences and DNA nanostructures, the use of multicolor fluorescent microdots significantly improves data writing/reading efficiency and reduces costs, making it more suitable for practical applications.

3.3. Fluorescent DNA Strand Encryption Based on DNA Sequences. In this study, data encryption and decryption are carried out through DNA strand displacement reactions on a solid-phase substrate. In the multicolor fluorescent storage system, the fluorescence on the DNA probes represents the stored data. Interference DNA strands, which are also fluorescently labeled, are added at specific

https://doi.org/10.1021/acsami.4c21723
ACS Appl. Mater. Interfaces 2025, 17, 10179−10190

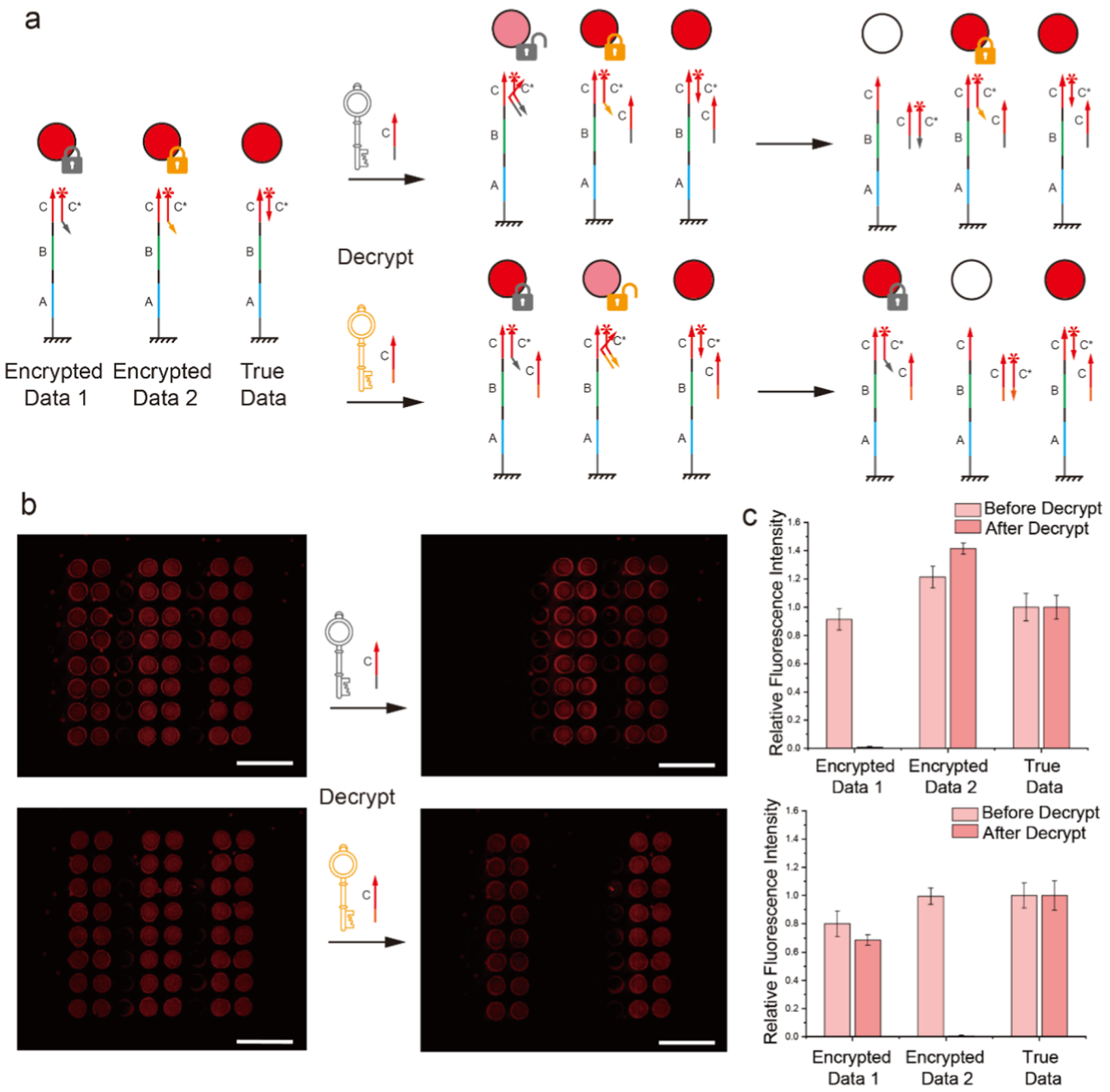


Figure 3. DNA strand displacement decryption based on DNA sequences. (a) Schematic representation of the encryption and decryption principles based on DNA strand displacement. Specific interference strands are removed only by the correct decryption strands, while data strands are retained during the decryption process. (b) Fluorescent dot array results of DNA strand displacement decryption (scale bar: 200 μm). (c) Relative fluorescence intensity results of DNA strand displacement decryption, using the intensity of the true data strand as the reference value (n = 8).

locations on the system to achieve data encryption. These interference DNA strands share the same backbone sequence as the data DNA strand, ensuring that they can hybridize to the support strand. However, the interference−interference DNA strands also contain a toehold sequence that does not hybridize with the support strand, allowing for their removal through the strand displacement process, thereby enabling decryption of the data. During the decryption process, a complementary decryption strand is introduced. This strand binds to the toehold of the interference DNA strand, facilitating its removal from the support strand through a strand displacement reaction. The DNA data strand, which lacks a complementary toehold sequence, remains intact during decryption. Due to the specificity of DNA hybridization and strand displacement, only the correct decryption strand can remove the corresponding interference DNA strand. Figure 3a illustrates the action of two interference DNA strands with different toehold sequences and their interaction with the data strand under different decryption strands. The interference DNA strand is only removed by the matching decryption strand, while the data DNA strand is retained after decryption. The experimental results are shown in Figure 3b,c. The corresponding decryption DNA solution was applied to the glass slides containing data DNA using a micropipette. A solid-phase

https://doi.org/10.1021/acsami.4c21723
ACS Appl. Mater. Interfaces 2025, 17, 10179−10190

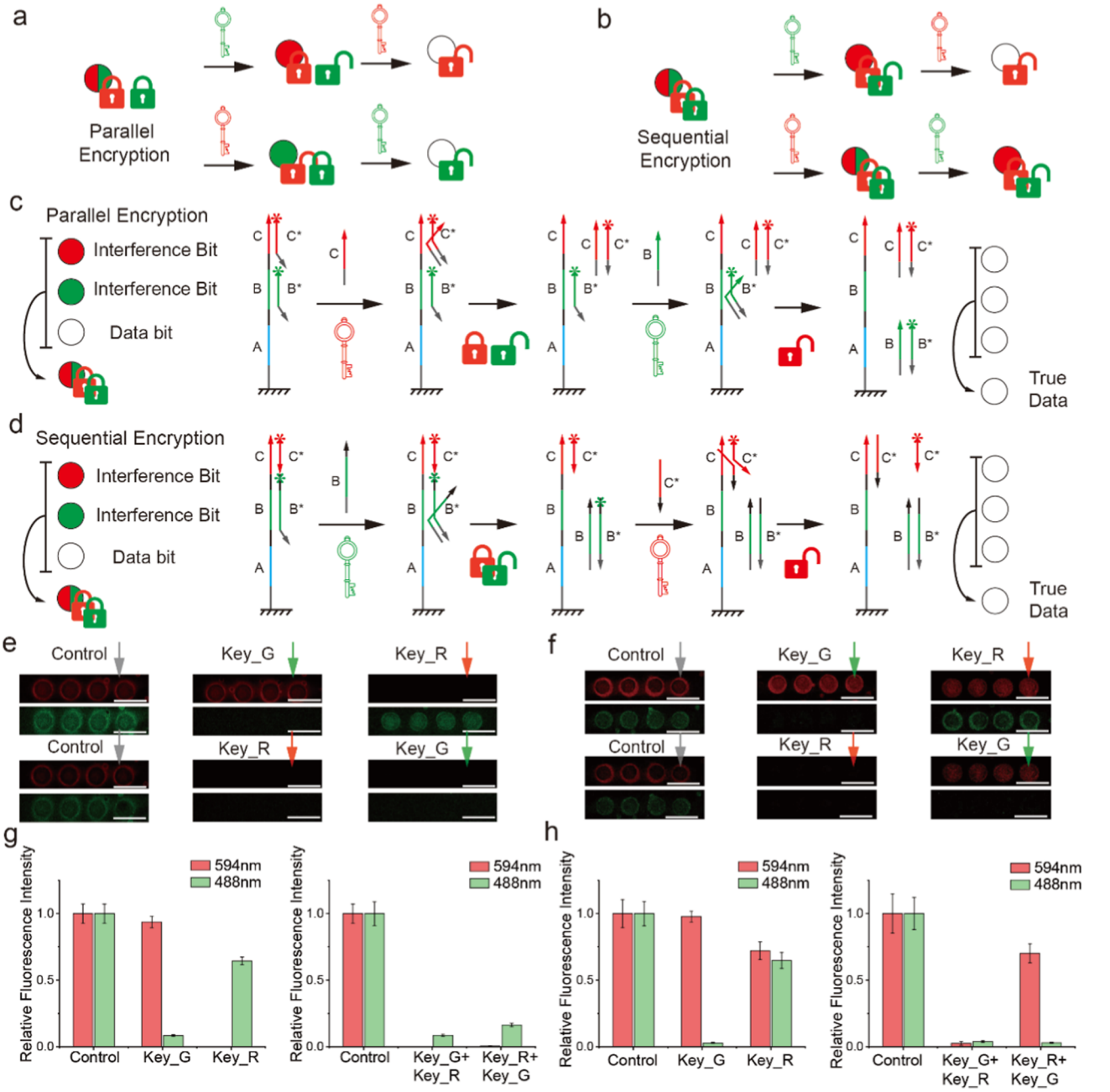


Figure 4. Multicolor DNA strand displacement encryption and decryption. (a) Illustration of the parallel encryption and decryption process. (b) Illustration of the sequential encryption and decryption process. (c) Schematic diagram of the principle of correct decryption for parallel encryption. (d) Schematic diagram of the principle of correct decryption for sequential encryption. (e) Fluorescence microscopy images of the parallel encryption and decryption process (scale bar: 100 μm). (f) Fluorescence microscopy images of the sequential encryption and decryption process (scale bar: 100 μm). (g) Relative fluorescence intensity results for parallel encryption and decryption, with the intensity of the buffer solution replacement control group as the standard (n = 8). (h) Relative fluorescence intensity results for sequential encryption and decryption, with the intensity of the buffer solution replacement control group as the standard (n = 8).

strand displacement reaction occurred at the interface between the solution and the glass slide, leading to the removal of the corresponding interference DNA strands. Fluorescence observation revealed a significant decrease in the intensity of the removed interference fluorescence compared with the other fluorescence signals. Because the washing process inevitably led to some fluorescence loss, the fluorescence change in this study is represented as the relative fluorescence intensity compared to the control group.

Since strand displacement requires tens of correct DNA base pairs to proceed, this encryption method offers excellent encryption depth. Moreover, this method may further enhance data security by erasing the correct data during an attack by unauthorized users. In the example shown in Figure 3, if DNA strand 2 also serves as an data strand, an attacker may mistakenly remove strand 2 as an interference strand during decryption attempts, thereby destroying part of the correct data. However, a user with the correct decryption key can

https://doi.org/10.1021/acsami.4c21723
ACS Appl. Mater. Interfaces 2025, 17, 10179−10190

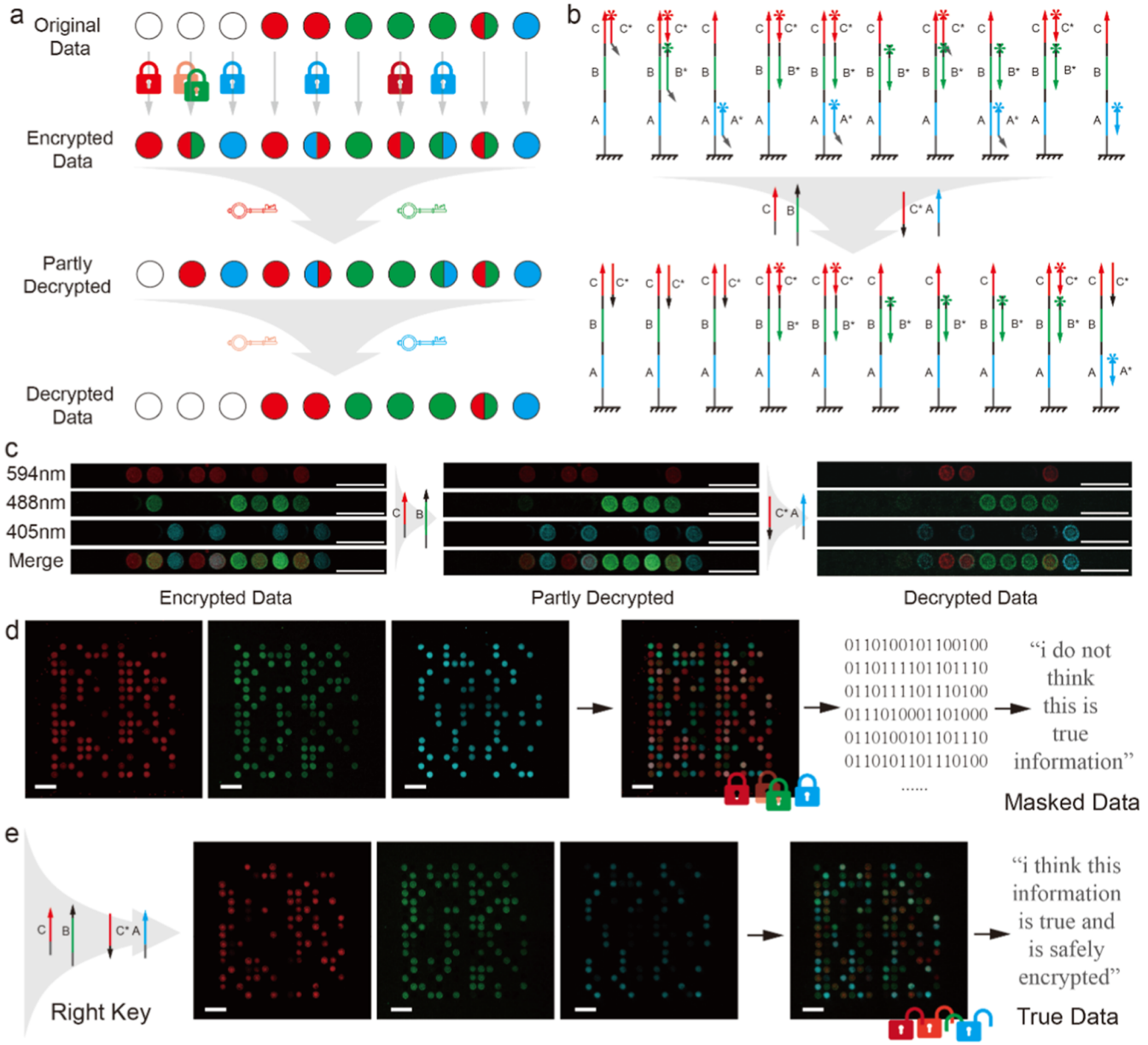


Figure 5. Demonstration of data encryption and decryption. (a) Encryption design: interference strands were introduced to blank points, single red points, and single green points for encryption. (b) Specific DNA structures for encryption. (c) Fluorescence results demonstration. Fluorescence microscopy revealed that as decryption strands were added sequentially, interference fluorescence dots were removed, leaving only the data fluorescence dots. (d) Without decryption, the fluorescent array produced masked data. (e) Applying the correct decryption strands allowed the fluorescent signals to be decoded into the true data.

precisely remove specific interference strands without affecting the data strands.

3.4. Multicolor Fluorescent DNA Strand Encryption Based on a Combinatorial Structure. Given that the support strand contains three hybridization regions, multiple regions can cooperatively participate in strand displacement to establish a more complex and secure encryption system. Previous research on DNA strand displacement has successfully demonstrated logic gates and even computational networks constructed by DNA molecules.[53−55] Inspired by these findings, this study also implements a similar combinatorial structure-based strand displacement system for multicolor fluorescence encryption through multistrand hybridization and displacement. Figure 4a,b shows two different encryption structures: parallel and sequential encryption. As shown in Figure 4c, two different hybridization regions on the support strand are encrypted independently using single-color encryption methods, as described in Section 3.3. This forms a parallel encryption scheme, where two distinct fluorescent interference strands are added separately and can be decrypted using their respective strands (Key_R for red fluorescence and Key_G for green fluorescence). In contrast, adjacent hybridization regions can enable coupled encryption, forming a sequential encryption scheme (Figure 4d). This method requires a sequential decryption process. It is noteworthy that unlike the previously described design, the interference DNA used in sequential encryption does not simply append a toehold to the end of the data DNA for removal. Specifically, the interference strand C* does not have a toehold; it is structurally identical to typical data DNA. To

https://doi.org/10.1021/acsami.4c21723
ACS Appl. Mater. Interfaces 2025, 17, 10179−10190

remove C*, a different decryption DNA must be used, which is complementary to the reaction region C and the adjacent spacer region in support DNA. This decryption DNA hybridizes with the support DNA, displacing the interference strand C* from region C, thus removing it. The corresponding interference strand B* has a toehold at its end, enabling its removal. The other end of B* contains an extended sequence that is complementary to the spacer region adjacent to the reaction region C, preventing the decryption DNA for C* from binding to the support DNA, thus protecting interference strand C*. Therefore, to decrypt this sequential encryption structure, the green decryption DNA (Key_G) must first be added to remove the green interference strand B*, followed by the red decryption DNA (Key_R) to remove the red interference strand C*, thus completing the decryption.

The experimental results for parallel encryption are shown in Figure 4e,g. Using "00000000" as the original data, red and green fluorescence interference DNA were added to form a parallel encryption structure. In the control group, the glass slide was first treated with blank buffer for the initial strand displacement followed by washing. A second strand displacement with a blank buffer was then performed, also followed by washing. The results indicated that washing caused a slight reduction in fluorescence intensity but the interference fluorescence was still clearly observable. In Experimental Group 1, Key_G was first added for strand displacement, and after washing, a significant reduction in green fluorescence was observed compared with the control group. Key_R was then added for strand displacement, and after washing, a significant reduction in the red fluorescence was observed. In Experimental Group 2, Key_R was added first for strand displacement and washing, followed by Key_G. The result showed that red fluorescence was reduced first and then green fluorescence was reduced. Thus, in parallel encryption, the order of decryption of DNA addition did not affect the decryption outcome. The experimental results for sequential encryption are shown in Figure 4f,h. Using "00000000" as the original data, red and green fluorescence interference DNA were added to form a sequential encryption structure. The control group was treated similarly to the parallel encryption group and received a similar result. In Experimental Group 1, Key_G was first added for strand displacement, and after washing, a significant reduction in green fluorescence was observed compared to the control group. Key_R was then added for strand displacement, and after washing, red fluorescence was significantly reduced, completing the correct decryption. In Experimental Group 2, Key_R was added first for strand displacement and washing, but fluorescence observation showed that red interference fluorescence was not reduced compared to the others. After Key_G was added for strand displacement and washing, green interference fluorescence was reduced but red fluorescence remained. Therefore, in sequential encryption, the decryption process must follow a specific order. Even with the correct decryption DNA, decryption will not be successful if the order is incorrect.

The encryption method utilizing multicolor strand displacement further demonstrates the potential of this system. The coupling between multiple DNA strands allows for the construction of specific computational reaction systems that form the foundation of an advanced encryption framework. In the sequential encryption, special interference DNA strands are introduced, which are identical to the data DNA in both sequence and fluorescence, with the only difference being the adjacent strands. Thus, even if a decryption key is obtained by an unauthorized user, the inability to fully understand the encryption mechanism will prevent the correct decryption of the encoded data.

Due to the limitations imposed by the solid-phase surface on DNA reactions, solid-phase DNA reactions differ from those in the liquid phase. They are also influenced by uncontrollable factors, such as surface charge, DNA attachment to the surface, and DNA morphology, making it challenging to construct an effective mathematical model. To ensure that the encryption system operates stably under different designs and external conditions, the system employs relatively high DNA concentrations as the reaction conditions. The results demonstrated that after the strand displacement reaction, the interference fluorescence is reduced by almost 80% compared to the data fluorescence. This significant difference ensures that decryption remains robust. Even if the initial conditions or reaction conditions are not precisely controlled to the optimal parameters, the substantial difference between interference and data fluorescence guarantees accurate data decryption.

3.5. Data Encryption Demonstration. The strand displacement encryption system demonstrated in this study can implement various encryption strategies with great flexibility. To validate its effectiveness, a specific encryption method combining parallel encryption and sequential encryption is employed, as shown in Figure 5a,b. Notably, in the sequential encryption structure, a special red interference DNA without a toehold was introduced. This interference DNA is identical in both sequence and fluorescence to the red data DNA, meaning that the corresponding decryption DNA could potentially displace the data DNA. To address this, a protection mechanism was introduced for the red data DNA in the encryption protocol to prevent its unintended removal. A protective sequence was added to the upstream region of the green DNA adjacent to the red DNA to safeguard the red data. In cases where a red data DNA is not adjacent to green data DNA, an additional nonfluorescent protective strand is introduced. The specific encryption rules are as follows: For data spots with no fluorescence, interference strands were randomly introduced, including red interference strands, red-green sequential interference structures, and blue interference strands. For data spots with only red fluorescence, a nonfluorescent "B" protection strand was added to form a sequential structure, preventing the removal of data strands by the decryption strand. Blue interference strands were then added to form a parallel structure. For spots with only green fluorescence, red or blue interference strands were randomly added to form a parallel structure. During decryption, green decryption keys (Key_G) and red decryption keys (Key_R1) were initially introduced to remove the green and some red interference strands. Subsequently, blue decryption keys (Key_B) and additional red decryption keys (Key_R2) were applied to remove blue interference strands and the remaining red interference strands, completing the decryption process. In the encryption strategy described above, Key_R1 and Key_R2 share 11 complementary bases. If both are introduced simultaneously, they could hybridize with each other, significantly compromising the strand displacement process. Therefore, to ensure the effectiveness of decryption, the four decryption strands are introduced in two separate steps during the strand displacement process.

First, this encryption was validated by spots (Figures 5c, S4 and S5). After the correct decryption DNA was added, the

https://doi.org/10.1021/acsami.4c21723
ACS Appl. Mater. Interfaces 2025, 17, 10179−10190

interference DNA was successfully removed, and the original data were restored. If only a subset of the correct keys is used, the structure of the encryption system will protect the data from being decrypted. For instance, introducing only the red decryption key would fail to remove all red interference strands because some are protected by the sequential structure. As a result, only the red interference DNA from the parallel encryption is removed (Figure S6). Since the red interference DNA is added randomly, even if the attacker observes that some strands are removed, they cannot discern any pattern, thus ensuring the data's security.

Based on the encryption and storage rules presented in this study, text data were encoded and verified (Figures 5 and S7). The encrypted fluorescent dot array was visualized under a fluorescence microscope, and decoding the ASCII-based dot array directly yielded masked data: "i do not think this is true data". When the correct decryption strands were applied, decoding the multicolor fluorescent signals produced the true data: "i think this data is true and is safely encrypted". If only partial correct decryption strands were introduced, then the outcome was garbage data (Figure S8). This demonstrates the robustness of the system against decryption attempts.

The stability of the encryption system relies on the stability of the DNA molecules. Therefore, extreme environmental conditions, such as high temperatures or extreme pH values, may indeed lead to DNA denaturation, which could affect the stability of the system. Existing literature provides ample evidence supporting the long-term stability of DNA molecules.[36,56,57] Under room temperature and dry conditions, the stability of the DNA molecules can support long-term storage. Specifically, a study by Kimberly et al. demonstrated that DNA duplexes, when dried on a solid-phase substrate, remain stable for up to 338 days at room temperature.[34] These duplexes can still undergo strand displacement reactions, and the displacement results can be distinguished by fluorescence. Thus, the storage system in this study should also support long-term storage under similar conditions at room temperature.

Overall, the encryption depth of this strategy is determined by the DNA sequences used for hybridization and the structural interactions among the multiple DNA strands. DNA strand displacement exhibits extremely high specificity, with kinetic processes sensitive to mismatches as small as a single nucleotide.[58] Research studies on genotyping have demonstrated that single-nucleotide mismatches in the toehold region can be effectively distinguished during strand displacement. Although mismatches within the hybridization region may be partially masked by correct sequences, the system maintains a high level of specificity overall.[59,60] When conventional 100 nt DNA strands are used, this encryption strategy achieves approximately 100 bits of quaternary encryption. The trial-and-error approach required to decipher such encryption demands an immense quantity of DNA synthesis time and financial resources. Moreover, combination structural interactions among multiple DNA encryption strands can necessitate the sequential addition of the correct decoding strands in a specific order. Failure to follow this order, even with the correct DNA strands, may result in incomplete decryption or even damage to the correct strands, leading to data loss.

4. CONCLUSIONS

This study introduces a DNA-based system for data storage and encryption. The system achieves solid-phase DNA hybridization and strand displacement at the microarray formed by inkjet printing, designing an encryption system governed by DNA sequences and combinatorial structures. DNA sequences possess an extremely high data storage density, providing remarkable encryption depth for secure data storage. Combinatorial structures between multiple encryption strands further enhance encryption complexity and flexibility, broadening encryption dimensions. Despite the high potential complexity of encryption mechanisms achievable with multicomponent DNA combinations, the implementation is straightforward and rapid by using inkjet printing. Inkjet printing allows the simultaneous deposition of diverse DNA strands into specific arrays quickly and cost-effectively. The decryption process, completed through simple DNA strand displacement, ensures an ease of data retrieval.

This system can be readily expanded to more versatile and flexible encryption functionalities through additional DNA combinations and design. As an emerging storage medium, DNA molecules boast unparalleled data density and are extensively studied in molecular computing. Applications of DNA have already extended to neural networks[54,61] and disease diagnosis.[62,63] Integrating DNA data storage and computational technologies with the inkjet-microarray-based solid-phase reaction system proposed in this work opens up new possibilities for storage and encryption.

■ ASSOCIATED CONTENT

Supporting Information

The Supporting Information is available free of charge at https://pubs.acs.org/doi/10.1021/acsami.4c21723.

Relationship between droplet size and fused microdroplets; methods for solid-phase DNA attachment; fluorescent design; micrographs of droplets printed in various experiments; relative fluorescence intensity results from encryption rule verification experiments; fluorescent microscopy results of incorrect decryption; and DNA sequence design (PDF)

Original data of the fluorescence results (XLSX)

■ AUTHOR INFORMATION

Corresponding Author

Zhuo Xiong − *Biomanufacturing Center, Department of Mechanical Engineering, Tsinghua University, Beijing 100084, China; Biomanufacturing and Rapid Forming Technology Key Laboratory of Beijing, Beijing 100084, China; Innovation International Talents Base (111 Base), Biomanufacturing and Engineering Living Systems, Beijing 100084, China;* orcid.org/0000-0002-9205-086X; Email: xiongzhuo@tsinghua.edu.cn

Authors

Ben Pei − *Biomanufacturing Center, Department of Mechanical Engineering, Tsinghua University, Beijing 100084, China; Biomanufacturing and Rapid Forming Technology Key Laboratory of Beijing, Beijing 100084, China; Innovation International Talents Base (111 Base), Biomanufacturing and Engineering Living Systems, Beijing 100084, China;* orcid.org/0000-0002-1433-1316

Jiaxiang Ma − *Biomanufacturing Center, Department of Mechanical Engineering, Tsinghua University, Beijing 100084, China; Biomanufacturing and Rapid Forming Technology Key Laboratory of Beijing, Beijing 100084,*

https://doi.org/10.1021/acsami.4c21723
ACS Appl. Mater. Interfaces 2025, 17, 10179−10190

China; Innovation International Talents Base (111 Base), Biomanufacturing and Engineering Living Systems, Beijing 100084, China

Liliang Ouyang − *Biomanufacturing Center, Department of Mechanical Engineering, Tsinghua University, Beijing 100084, China; Biomanufacturing and Rapid Forming Technology Key Laboratory of Beijing, Beijing 100084, China; Innovation International Talents Base (111 Base), Biomanufacturing and Engineering Living Systems, Beijing 100084, China;* orcid.org/0000-0003-4177-8698

Complete contact information is available at: https://pubs.acs.org/10.1021/acsami.4c21723

Author Contributions

Zhuo Xiong designed the experiments and supervised the projects. Ben Pei prepared the materials and performed the experiments. Jiaxiang Ma prepared the inkjet experiments. Liliang Ouyang supervised the inkjet experiments. Ben Pei wrote the original manuscript and finished the final version. The manuscript was written through the contributions of all authors, and all authors have given approval of the final version of the manuscript.

Notes

The authors declare no competing financial interest.

■ ACKNOWLEDGMENTS

This work was funded by the new faculty start-up funding provided by Tsinghua University (53330200321, Z.X.).

■ REFERENCES

(1) Wu, Y.; Chen, X.; Wu, W. Multiple Stimuli-Response Polychromatic Carbon Dots for Advanced Information Encryption and Safety. *Small* **2023**, *19* (10), No. e2206709.

(2) Gao, Y.; Ge, K.; Zhang, Z.; Li, Z.; Hu, S.; Ji, H.; Li, M.; Feng, H. Fine Optimization of Colloidal Photonic Crystal Structural Color for Physically Unclonable Multiplex Encryption and Anti-Counterfeiting. *Adv. Sci. (Weinh)* **2024**, *11* (20), No. e2305876.

(3) Dai, X.-Y.; Huo, M.; Liu, Y. Phosphorescence resonance energy transfer from purely organic supramolecular assembly. *Nat. Rev. Chem* **2023**, *7* (12), 854−874.

(4) Hou, J.; Li, M.; Song, Y. Patterned Colloidal Photonic Crystals. *Angew. Chem., Int. Ed.* **2018**, *57* (10), 2544−2553.

(5) Hong, W.; Yuan, Z.; Chen, X. Structural Color Materials for Optical Anticounterfeiting. *Small* **2020**, *16* (16), No. e1907626.

(6) Yang, Z.; Xu, T.; Li, H.; She, M.; Chen, J.; Wang, Z.; Zhang, S.; Li, J. Zero-Dimensional Carbon Nanomaterials for Fluorescent Sensing and Imaging. *Chem. Rev.* **2023**, *123* (18), 11047−11136.

(7) Sardari, N.; Abdollahi, A.; Farokhi Yaychi, M. Chameleon-like Photoluminescent Janus Nanoparticles as Full-Color Multicomponent Organic Nanoinks: Combination of Forster Resonance Energy Transfer and Photochromism for Encryption and Anticounterfeiting with Multilevel Authentication. *ACS Appl. Mater. Interfaces* **2023**, *15* (49), 57656−57678.

(8) Kumar, P.; Singh, S.; Gupta, B. K. Future prospects of luminescent nanomaterial based security inks: from synthesis to anti-counterfeiting applications. *Nanoscale* **2016**, *8* (30), 14297−14340.

(9) Song, B.; Wang, H.; Zhong, Y.; Chu, B.; Su, Y.; He, Y. Fluorescent and magnetic anti-counterfeiting realized by biocompatible multifunctional silicon nanoshuttle-based security ink. *Nanoscale* **2018**, *10* (4), 1617−1621.

(10) Khlifi, S.; Fournier Le Ray, N.; Paofai, S.; Amela-Cortes, M.; Akdas-Kiliç, H.; Taupier, G.; Derien, S.; Cordier, S.; Achard, M.; Molard, Y. Self-erasable inkless imprinting using a dual emitting hybrid organic-inorganic material. *Mater. Today* **2020**, *35*, 34−41.

(11) Abdollahi, A.; Roghani-Mamaqani, H.; Razavi, B.; Salami-Kalajahi, M. Photoluminescent and Chromic Nanomaterials for Anticounterfeiting Technologies: Recent Advances and Future Challenges. *ACS Nano* **2020**, *14* (11), 14417−14492.

(12) Abdollahi, A.; Roghani-Mamaqani, H.; Razavi, B. Stimuli-chromism of photoswitches in smart polymers: Recent advances and applications as chemosensors. *Prog. Polym. Sci.* **2019**, *98*, 101149.

(13) Liu, S.; Liu, X.; Zhu, X.; Yin, J.; Bao, J. Multiple-Channel Information Encryption Based on Quantum Dot Absorption Spectra. *ACS Nano* **2023**, *17* (21), 21349−21359.

(14) Abdollahi, A.; Roghani-Mamaqani, H.; Razavi, B.; Salami-Kalajahi, M. The light-controlling of temperature-responsivity in stimuli-responsive polymers. *Polym. Chem.* **2019**, *10* (42), 5686−5720.

(15) Bai, L.; Xie, Z.; Wang, W.; Yuan, C.; Zhao, Y.; Mu, Z.; Zhong, Q.; Gu, Z. Bio-inspired vapor-responsive colloidal photonic crystal patterns by inkjet printing. *ACS Nano* **2014**, *8* (11), 11094−11100.

(16) Liu, Y.; Zhang, Y. Moving Binary-Color Heterojunction for Spatiotemporal Multilevel Encryption via Directional Swelling and Anion Exchange. *ACS Nano* **2021**, *15* (4), 7628−7637.

(17) Zhang, Y. C.; Le, X. X.; Jian, Y. K.; Lu, W.; Zhang, J. W.; Chen, T. 3D Fluorescent Hydrogel Origami for Multistage Data Security Protection. *Adv. Funct. Mater.* **2019**, *29* (46), 1905514.

(18) Otaegui, J. R.; Ruiz-Molina, D.; Hernando, J.; Roscini, C. Multidimensional Data Encoding Based on Multicolor Microencapsulated Thermoresponsive Fluorescent Phase Change Materials. *Adv. Funct. Mater.* **2024**, *34* (34), 2402510.

(19) Li, Z.; Liu, Y.; Zhang, C.; Qiao, Y.; Deng, R.; Shi, Y.; Li, Z.; Liu, Q.; Zhang, Z. B.; Li, H. Z.; Song, Y. L. On-Chip Direction-Multiplexed Meta-Optics for High-Capacity 3D Holography. *Adv. Funct. Mater.* **2024**, *34* (16), 2312705.

(20) Ko, B.; Badloe, T.; Yang, Y.; Park, J.; Kim, J.; Jeong, H.; Jung, C.; Rho, J. Tunable metasurfaces via the humidity responsive swelling of single-step imprinted polyvinyl alcohol nanostructures. *Nat. Commun.* **2022**, *13* (1), 6256.

(21) Zhang, Y.; Yu, Z.; Qu, H.; Guo, S.; Yang, J.; Zhang, S.; Yang, L.; Cheng, S.; Wang, J.; Tan, S. C. Self-Sustained Programmable Hygroelectronic Interfaces for Humidity-Regulated Hierarchical Information Encryption and Display. *Adv. Mater.* **2024**, *36* (12), No. e2208081.

(22) Shen, J.; Xiao, Q.; Sun, P.; Feng, J.; Xin, X.; Yu, Y.; Qi, W. Self-Assembled Chiral Phosphorescent Microflowers from Au Nanoclusters with Dual-Mode pH Sensing and Information Encryption. *ACS Nano* **2021**, *15* (3), 4947−4955.

(23) Wang, Q.; Qi, Z.; Wang, Q. M.; Chen, M.; Lin, B. Y.; Qu, D. H. A Time-Dependent Fluorescent Hydrogel for "Time-Lock" Information Encryption. *Adv. Funct. Mater.* **2022**, *32* (49), 2208865.

(24) Ding, L.; Wang, X. D. Luminescent Oxygen-Sensitive Ink to Produce Highly Secured Anticounterfeiting Labels by Inkjet Printing. *J. Am. Chem. Soc.* **2020**, *142* (31), 13558−13564.

(25) Zhao, Y. J.; Zhao, H.; Di, Y. S.; Liu, C. H.; Xing, F. J.; Wen, X. M.; Jia, B. H.; Gan, Z. X. Double-Key Optical Information Encryption Enabled by Multi-State Excitation-Emission of Mn-Doped Metal Chlorides. *Adv. Opt. Mater.* **2023**, *11* (19), 2301349.

(26) Zheng, H. Q.; Yang, Y.; Wang, Z.; Yang, D.; Qian, G.; Cui, Y. Photo-Stimuli-Responsive Dual-Emitting Luminescence of a Spiropyran-Encapsulating Metal-Organic Framework for Dynamic Information Encryption. *Adv. Mater.* **2023**, *35* (26), No. e2300177.

(27) Singh, A. K.; Singh, S.; Gupta, B. K. Highly Efficient, Chemically Stable, and UV/Blue-Light-Excitable Biluminescent Security Ink to Combat Counterfeiting. *ACS Appl. Mater. Interfaces* **2018**, *10* (51), 44570−44575.

(28) Zhang, Y.; Ren, Y.; Liu, Y.; Wang, F.; Zhang, H.; Liu, K. Preservation and Encryption in DNA Digital Data Storage. *ChemPlusChem* **2022**, *87* (9), No. e202200183.

(29) Goldman, N.; Bertone, P.; Chen, S.; Dessimoz, C.; LeProust, E. M.; Sipos, B.; Birney, E. Towards practical, high-capacity, low-maintenance information storage in synthesized DNA. *Nature* **2013**, *494* (7435), 77−80.

(30) Church, G. M.; Gao, Y.; Kosuri, S. Next-generation digital information storage in DNA. *Science* **2012**, *337* (6102), 1628.
(31) Wang, S.; Mao, X.; Wang, F.; Zuo, X.; Fan, C. Data Storage Using DNA. *Adv. Mater.* **2024**, *36* (6), No. e2307499.
(32) Ceze, L.; Nivala, J.; Strauss, K. Molecular digital data storage using DNA. *Nat. Rev. Genet.* **2019**, *20* (8), 456−466.
(33) Fan, S.; Wang, D.; Cheng, J.; Liu, Y.; Luo, T.; Cui, D.; Ke, Y.; Song, J. Information Coding in a Reconfigurable DNA Origami Domino Array. *Angew. Chem., Int. Ed. Engl.* **2020**, *59* (31), 12991−12997.
(34) Berk, K. L.; Blum, S. M.; Funk, V. L.; Sun, Y.; Yang, I. Y.; Gostomski, M. V.; Roth, P. A.; Liem, A. T.; Emanuel, P. A.; Hogan, M. E.; Miklos, A. E.; Lux, M. W. Rapid Visual Authentication Based on DNA Strand Displacement. *ACS Appl. Mater. Interfaces* **2021**, *13* (16), 19476−19486.
(35) Zhu, E.; Luo, X.; Liu, C.; Chen, C. An Operational DNA Strand Displacement Encryption Approach. *Nanomaterials (Basel)* **2022**, *12* (5), 877.
(36) Simmel, F. C.; Yurke, B.; Singh, H. R. Principles and Applications of Nucleic Acid Strand Displacement Reactions. *Chem. Rev.* **2019**, *119* (10), 6326−6369.
(37) Song, Y.; Kim, S.; Heller, M. J.; Huang, X. DNA multi-bit non-volatile memory and bit-shifting operations using addressable electrode arrays and electric field-induced hybridization. *Nat. Commun.* **2018**, *9* (1), 281.
(38) Yang, S.; Boegels, B. W. A.; Wang, F.; Xu, C.; Dou, H. J.; Mann, S.; Fan, C. H.; de Greef, T. F. A. DNA as a universal chemical substrate for computing and data storage. *Nat. Rev. Chem* **2024**, *8* (3), 179−194.
(39) Polak, R. E.; Keung, A. J. A molecular assessment of the practical potential of DNA-based computation. *Curr. Opin. Biotechnol.* **2023**, *81*, 102940.
(40) Lapteva, A. P.; Sarraf, N.; Qian, L. DNA Strand-Displacement Temporal Logic Circuits. *J. Am. Chem. Soc.* **2022**, *144* (27), 12443−12449.
(41) Lakin, M. R.; Stefanovic, D. Supervised Learning in Adaptive DNA Strand Displacement Networks. *ACS Synth. Biol.* **2016**, *5* (8), 885−897.
(42) Song, T.; Eshra, A.; Shah, S.; Bui, H.; Fu, D.; Yang, M.; Mokhtar, R.; Reif, J. Fast and compact DNA logic circuits based on single-stranded gates using strand-displacing polymerase. *Nat. Nanotechnol.* **2019**, *14* (11), 1075−1081.
(43) Gunina, E. V.; Gorbunova, I.; Rzhevskiy, S.; Kenzhebayeva, Y.; Bachinin, S.; Shipilovskikh, D.; Mitusova, K.; Rogova, A.; Kulakova, A. N.; Timin, A. S.; Shipilovskikh, S.; Milichko, V. A. Inkjet Printing of Biocompatible Luminescent Organic Crystals for Optical Encryption. *ACS Appl. Opt. Mater.* **2023**, *1* (12), 2013−2020.
(44) Wang, M.; Jiang, K.; Gao, Y.; Liu, Y.; Zhang, Z.; Zhao, W.; Ji, H.; Zheng, T.; Feng, H. A facile fabrication of conjugated fluorescent nanoparticles and micro-scale patterned encryption via high resolution inkjet printing. *Nanoscale* **2021**, *13* (34), 14337−14345.
(45) Li, X.; Liu, B.; Pei, B.; Chen, J.; Zhou, D.; Peng, J.; Zhang, X.; Jia, W.; Xu, T. Inkjet Bioprinting of Biomaterials. *Chem. Rev.* **2020**, *120* (19), 10793−10833.
(46) Bietsch, A.; Hegner, M.; Lang, H. P.; Gerber, C. Inkjet deposition of alkanethiolate monolayers and DNA oligonucleotides on gold: evaluation of spot uniformity by wet etching. *Langmuir* **2004**, *20* (12), 5119−5122.
(47) Saaem, I.; Ma, K. S.; Marchi, A. N.; LaBean, T. H.; Tian, J. In situ synthesis of DNA microarray on functionalized cyclic olefin copolymer substrate. *ACS Appl. Mater. Interfaces* **2010**, *2* (2), 491−497.
(48) Park, J. U.; Lee, J. H.; Paik, U.; Lu, Y.; Rogers, J. A. Nanoscale patterns of oligonucleotides formed by electrohydrodynamic jet printing with applications in biosensing and nanomaterials assembly. *Nano Lett.* **2008**, *8* (12), 4210−4216.
(49) Shah, M. A.; Lee, D. G.; Lee, B. Y.; Hur, S. Classifications and Applications of Inkjet Printing Technology: A Review. *IEEE Access* **2021**, *9*, 140079−140102.
(50) Zub, K.; Hoeppener, S.; Schubert, U. S. Inkjet Printing and 3D Printing Strategies for Biosensing, Analytical, and Diagnostic Applications. *Adv. Mater.* **2022**, *34* (31), No. e2105015.
(51) Xu, J.; Wang, Y.; Chen, X.; Wang, L.; Zhou, H.; Mei, H.; Chen, S.; Huang, X. Multi-layer encryption of medical data in DNA for highly-secure storage. *Mater. Today Bio* **2024**, *28*, 101221.
(52) Jiang, C.; Tan, R.; Li, W.; Zhang, Y.; Liu, H. Subtraction-based DNA Origami Cryptography by using Structural Defects for Information Encryption. *Small* **2024**, *20* (51), No. e2406470.
(53) Qian, L.; Winfree, E. Scaling up digital circuit computation with DNA strand displacement cascades. *Science* **2011**, *332* (6034), 1196−1201.
(54) Okumura, S.; Gines, G.; Lobato-Dauzier, N.; Baccouche, A.; Deteix, R.; Fujii, T.; Rondelez, Y.; Genot, A. J. Nonlinear decision-making with enzymatic neural networks. *Nature* **2022**, *610* (7932), 496−501.
(55) Wang, F.; Lv, H.; Li, Q.; Li, J.; Zhang, X.; Shi, J.; Wang, L.; Fan, C. Implementing digital computing with DNA-based switching circuits. *Nat. Commun.* **2020**, *11* (1), 121.
(56) Matange, K.; Tuck, J. M.; Keung, A. J. DNA stability: a central design consideration for DNA data storage systems. *Nat. Commun.* **2021**, *12* (1), 1358.
(57) Chen, W. D.; Kohll, A. X.; Nguyen, B. H.; Koch, J.; Heckel, R.; Stark, W. J.; Ceze, L.; Strauss, K.; Grass, R. N. Combining Data Longevity with High Storage Capacity—Layer-by-Layer DNA Encapsulated in Magnetic Nanoparticles. *Adv. Funct. Mater.* **2019**, *29* (28), 1901672.
(58) Khodakov, D. A.; Khodakova, A. S.; Huang, D. M.; Linacre, A.; Ellis, A. V. Protected DNA strand displacement for enhanced single nucleotide discrimination in double-stranded DNA. *Sci. Rep.* **2015**, *5*, 8721.
(59) Khodakov, D. A.; Khodakova, A. S.; Linacre, A.; Ellis, A. V. Toehold-mediated nonenzymatic DNA strand displacement as a platform for DNA genotyping. *J. Am. Chem. Soc.* **2013**, *135* (15), 5612−5619.
(60) Knez, K.; Spasic, D.; Janssen, K. P.; Lammertyn, J. Emerging technologies for hybridization based single nucleotide polymorphism detection. *Analyst* **2014**, *139* (2), 353−370.
(61) Cherry, K. M.; Qian, L. Scaling up molecular pattern recognition with DNA-based winner-take-all neural networks. *Nature* **2018**, *559* (7714), 370−376.
(62) Yang, L.; Tang, Q.; Zhang, M.; Tian, Y.; Chen, X.; Xu, R.; Ma, Q.; Guo, P.; Zhang, C.; Han, D. A spatially localized DNA linear classifier for cancer diagnosis. *Nat. Commun.* **2024**, *15* (1), 4583.
(63) Ma, Q.; Zhang, M.; Zhang, C.; Teng, X.; Yang, L.; Tian, Y.; Wang, J.; Han, D.; Tan, W. An automated DNA computing platform for rapid etiological diagnostics. *Sci. Adv.* **2022**, *8* (47), No. eade0453.

https://doi.org/10.1021/acsami.4c21723
ACS Appl. Mater. Interfaces 2025, 17, 10179−10190