High-Content Optical Codes for Protecting Rapid Diagnostic Tests from Counterfeiting

Onur Gökçe,* Cristina Mercandetti, and Emmanuel Delamarche*©
IBM Research, Zurich, 8803 Rüschlikon Switzerland

ABSTRACT: Warnings and reports on counterfeit diagnostic devices are released several times a year by regulators and public health agencies. Unfortunately, mishandling, altering, and counterfeiting point-of-care diagnostics (POCDs) and rapid diagnostic tests (RDTs) is lucrative, relatively simple and can lead to devastating consequences. Here, we demonstrate how to implement optical security codes in silicon- and nitrocellulose-based flow paths for device authentication using a smartphone. The codes are created by inkjet spotting inks directly on nitrocellulose or on micropillars. Codes containing up to 32 elements per mm² and 8 colors can encode as many as 10⁴⁵ combinations. Codes on silicon micropillars can be erased by setting a continuous flow path across the entire array of code elements or for nitrocellulose by simply wicking a liquid across the code. Static or labile code elements can further be formed on nitrocellulose to create a hidden code using poly(ethylene glycol) (PEG) or glycerol additives to the inks. More advanced codes having a specific deletion sequence can also be created in silicon microfluidic devices using an array of passive routing nodes, which activate in a particular, programmable sequence. Such codes are simple to fabricate, easy to view, and efficient in coding information; they can be ideally used in combination with information on a package to protect diagnostic devices from counterfeiting.

Infectious diseases claimed 8.23 million lives in 2016, mostly from the developing world. An estimated 1.2 million deaths from malaria, tuberculosis, syphilis, and pneumonia could have been prevented with adequate diagnostics, but unfortunately, 70% of Africa and 40% of Asia did not have access to sufficient infrastructure (electricity, clean water, physical infrastructure, skilled staff) to run clinical tests. This is why POCDs, and in particular low-cost, simple-to-fabricate, and simple-to-operate RDTs had a significant impact on global health in detecting diseases in resource-limited settings, mapping infectious diseases, reducing presumptive treatments, and screening blood before donation and transfusion. Not surprisingly, the adoption of RDTs is increasing worldwide with the help of internationally funded programs.

Unfortunately, RDTs also attracted the attention of criminals who started to inject poor-quality products into the market. As an example, the World Health Organization (WHO) reported that counterfeit RDTs for visceral leishmaniasis started to circulate in the Indian subcontinent soon after an elimination initiative against visceral leishmaniasis was started there. The WHO estimates that more than 8% of the medical devices in circulation in 2010 were counterfeit. This figure is expected to increase, in part because of the growing importance of “online pharmacies”.

Counterfeit RDTs are typically nonfunctional products mimicking the look of genuine tests. They can also consist of genuine tests with falsified labels and expiration dates. For example, pregnancy tests were labeled as HIV tests and sold to blood banks in West Bengal, expired HIV tests were resold in Kinshasa with altered expiration dates, and fake ebola diagnostic kits appeared in Lagos during the 2014 outbreak before genuine ebola RDTs ever existed. Counterfeit RDTs kill individuals and contribute to the spreading of infectious diseases due to misdiagnosis. They also foster mistrust in health-care workers, who may stop relying on valid test results. Today’s fragmented and complex global supply chains further challenge the viability of RDTs, which frequently experience mishandling during distribution and storage. Their availability can be sporadic, sometimes with a limited supply and at other times in excess, resulting in tests that expire in storage.

These alarming facts call for a widespread adoption of strong and low-cost security features for authenticating and tracking RDTs. Currently, the two main strategies used in the healthcare industry against counterfeiting are (1) “security printing”, which consists of methods to create hard-to-replicate security features such as holograms or tags with special inks, and (2) “digital tagging”, where the information stored in digital tags...
provides the security. Features produced by security printing tend to be copied over time. Holograms, for example, can be reproduced at low quality without a lay person noticing it. Hard-to-fabricate security tags, such as photonic and plasmonic micro/nanostructures, can be integrated into microfabricated RDTs, but these tags typically require expensive and time-consuming fabrication processes, which makes it challenging to label each product with a unique tag. Digital tagging is a promising approach for securing RDTs because a large security code (a couple of kilobytes) that is unique for each product can be stored on low-cost RFID chips or simply printed as QR codes. These codes can be read and crosschecked using the Internet or a cellular network. The EU directive on falsified medicines will require all drugs to be labeled on their packages with unique identification tags by February 2019. The FDA global unique device identification database will similarly require all medical products to be individually labeled by September 2018. However, security features on a package secure the package, not necessarily the product it contains. Scavenged packages from used products have been used to repack counterfeit medical products. Additionally, security features on packages are exposed and can be copied anywhere in the supply chain.

A stronger security can be achieved by embedding a digital security code in the functional component of a product, which cannot be transferred to counterparts. This approach was recently demonstrated by different groups using different methods. Scherr et al. patterned control antibodies on a nitrocellulose membrane to create a QR code that appeared when the diagnostic test was run. This method however required a large area for the QR code (12.5 × 12.5 mm²), did not allow to authenticate a device before using it, and antibodies used as code generating molecules might be expensive. In a similar method, Park et al. patterned DNA probes on a DNA microarray chip to produce a QR code upon hybridization with complementary fluorescent probes. Han et al. placed fluorescent polymer microtags carrying QR codes inside individual drug capsules, but the drug capsule had to be destroyed in order to access the code. Ciftlik et al. imprinted fluorescent QR codes in a parylene-C bonding layer in microfluidic chips using UV irradiation. This technology has a high precision capability but is limited to chips packaged using parylene-C.

Our approach on securing RDTs is based on introducing unique and compact optical security codes into microfluidic devices or on nitrocellulose flow paths. We specifically focus on implementing static and dynamic codes where reading the code before or during a test provides sufficient complexity when complemented with a QR code on a package. The optical codes are easy to write with an inkjet spotter using low-cost dyes and easy to decode using a smartphone equipped with a simple clip-on macro lens. The strategy can allow authenticating RDTs with or without network connectivity (Figure 1). With intermittent or continuous connectivity, devices can be tracked through the supply chain, their use can be logged or incidents may be reported to regulators.

**EXPERIMENTAL SECTION**

**Materials and Software.** Water deionized using a Millipore system was used for all inks. Inks contained either 10% PEG (molecular weight: 3000, Sigma-Aldrich) or 20% (w:v) glycerol (Sigma-Aldrich) in addition to amaranth (providing a magenta-like color, Sigma-Aldrich), brilliant blue FCF (providing a cyan-like color, Sigma-Aldrich), tartrazine (yellow, Sigma-Aldrich), or brilliant black BN (Sigma-Aldrich) dyes. Inks for the codes on Si micropillars contained 20 mg mL⁻¹ amaranth or 10 mg mL⁻¹ brilliant blue FCF. Inks for nitrocellulose membrane (BioTrace NT, pore size: 0.2 μm, Pall Life Sciences) contained 10 mg mL⁻¹ amaranth, 3.3 mg mL⁻¹ brilliant blue FCF, or 20 mg mL⁻¹ tartrazine. The ink deposited on the 3D microfluidic device for multiple deletion steps contained 1.0 mg mL⁻¹ brilliant black BN. The Si microfluidic chips were filled with an aqueous 0.1% (w:v) Tween-20 (Sigma-Aldrich) solution. The nitrocellulose membrane was wetted with an aqueous 0.1% sodium dodecyl sulfate (SDS, Fluka) solution in experiments involving the deletion of code elements.

![Figure 1](image-url)
Images were captured using a digital camera (Leica MC170 HD) attached to a stereoscopic microscope (Leica MX16), and processed using Fiji for brightness and contrast. Data analysis and graphs were done using Matlab.

The protocol for validating optical codes was implemented (1) for the client application in JavaScript to run on the web browsers of smartphones and (2) for the server in Python using Flask microframework running on a cloud service (Bluemix).

**Fabrication.** The microfluidic chips were fabricated on Si wafers having 600 nm-thick thermally grown SiO₂ oxide layer using standard photolithography and deep reactive-ion etching (DRIE, Figure 2c). Briefly, the microchannels were patterned on the oxide layer using a 1.2-μm resist (AZ 6612) and glass/chromium masks. The photoresist layer was etched using DRIE and the oxide layer as a mask. Finally, the processed wafers were diced (ESEC 8803 Dicing Saw). The quality of the fabrication was verified using various items (encoded numbers, text, checker pattern) and 2 alignment marks. (c) Fabrication steps for creating the code on Si micropillars using standard optical lithography, etching, inkjet spotting, and lamination techniques.

![Image 2](https://example.com/image2.png)

**Figure 2.** Implementation of static optical security codes on microstructures, which can be patterned inside microfluidic chips. (a) Droplets of ink are inkjet spotted on micropillars to create single code elements after drying, as seen in the SEM image. (b) Microscope image showing a multicolor code composed of 14 x 14 elements and displaying various items (encoded numbers, text, checker pattern) and 2 alignment marks. (c) Fabrication steps for creating the code on Si micropillars using standard optical lithography, etching, inkjet spotting, and lamination techniques.

In the fabrication of the 3D microfluidic chips was similar except for an additional photolithography and DRIE process to fabricate the bottom microfluidic layer at the back side of 400-μm-thick wafers. The microfluidic layers were formed by etching 20 μm using DRIE. The vias were opened by etching through the wafer. After fabrication, the chips were laminated for 2 min using 0.1% (v/v) trichloro(octyl)silane (Sigma-Aldrich).

In heptane (Sigma-Aldrich). The chips were sealed with 3 mm-thick layers of polydimethylsiloxane (PDMS, Dow Corning Sylgard 184) prior to use. A syringe pump (Kent Scientific Genie) was used to fill these devices with water at a rate of 1.5 μL min⁻¹.

**Inkjet Spotting.** The reagents were deposited using a NanoPlotter 2.1 inkjet spotter equipped with a NanoTip J piezoelectric pipetting tip (GeSiM, Dresden). The spotter was controlled using a custom spotting program. Prior to spotting inks, the exact position of the Si chips on the tray of the inkjet spotter needed to be determined for precise targeting of the ink onto Si micropillars. This was done by spotting test spots on two grids placed at the opposite ends of the Si chip and measuring the lateral offset of the test spots. The height of the target surfaces was measured with the tactile Z-sensor supplied with the spotter. Spotting was done at a distance of 0.25 mm from the Si surface, or 0.5 mm from the nitrocellulose membrane. The piezoelectric tips were actuated using 60 to 90 V amplitude and 20 to 50 μs pulse width. The deposition rate was 100 Hz for spotting on Si and 1000 Hz for the nitrocellulose membrane.

The volume of dispensed droplets was characterized by measuring their diameter using a stereoscopic image and found to be 386 ± 64 pL. Single droplets of ink containing PEG were deposited on Si micropillars. Inks containing PEG or glycerol were deposited in 20 or 5 droplets respectively on the nitrocellulose membrane to generate the code elements with primary colors. Thirty or 8 additional droplets of a second ink containing PEG or glycerol were spotted over the primary colors to generate the code elements with secondary colors (green, purple, red).

The error rate associated with placing code elements on micropillars was characterized by spotting single droplets of amaranth ink containing PEG on an array of micropillars and subsequently counting uncoated ones.

**Analysis of Code Properties.** In dynamic codes that are partially deleted (e.g., Figures 4 and 5), the remaining code comprises a subset of the initial code elements. Therefore, for a dynamic code with n code elements of which k of them are set, the remaining code can have k code elements of which l of them can be set. The total number of codes, \( S_{\text{par}}(n) \), that can be written with this scheme is

\[
S_{\text{par}}(n) = \sum_{k=0}^{n} \left( \binom{n}{k} \sum_{l=0}^{k} \binom{k}{l} \right)
\]

which simplifies to \( S_{\text{par}}(n)=3^{n} \). Therefore, codes with partial deletion have an equivalent capacity of \( \log_2 S_{\text{par}}(n) = n \log_2 3 \) bits.

Deleting the code in multiple steps (e.g., Figures 5 and 6) adds \( \log_2 D(b) \) extra bits to the capacity of the code, where \( D(b) \) is the number of different ways to delete the code in b deletion steps. \( D(b) \) can be represented in a recursive function

\[
D(b) = 2 + \sum_{d=1}^{b-1} \binom{b}{d} D(b - d)
\]

for \( b > 0 \), where \( D(0) = 0 \) and \( d \) is the number of nodes activated simultaneously in one deletion step. The total number of nodes that need to be activated to achieve \( D(b) \) different deletions is
Analytical Chemistry

\[ S_{\text{node}}(b) = b + \sum_{d=1}^{b-1} \left( \binom{b}{d} D(b-d) + S_{\text{node}}(b-d) \right) \]

for \( b \geq 0 \). Then, the total number of spots to write all of the possible codes with \( n \) code elements and \( \beta \) deletion steps is

\[ S_{\text{spot}}(n, \beta) = \sum_{k=0}^{n} \binom{n}{k} D(b) + S_{\text{node}}(b) \]

Assuming that patterning each spot takes \( t_{\text{spot}} \) amount of time to move the inkjet head and to deposit the dye, the average time to write a code is the time it takes to write all possible codes divided by the total number of writable codes

\[ T_{\text{code}}(n, \beta) = \frac{t_{\text{spot}} S_{\text{spot}}(n, \beta)}{\sum_{k=0}^{n} \binom{n}{k} D(b)} \]

Dynamic codes with multistep deletion implemented as shown in Figure 6 require extra area for the array of nodes that has a size of \( b \times (b+1) \) nodes. The total footprint of these dynamic codes, \( A_{\text{total}}(n, \beta) \), can be approximated as

\[ A_{\text{total}}(n, \beta) = n A_{\text{bit}} + (b^2 + b) A_{\text{node}} \]

where \( A_{\text{bit}} \) is the area occupied by 1 code element and \( A_{\text{node}} \) is by 1 node.

**RESULTS AND DISCUSSION**

**Optical Codes Formed with an Array of Micropillars in Silicon.** A 2D array of code elements, which can be seen by eye or using a simple optical reader, is an efficient and widespread approach to providing information for the authentication of products. We chose to form such code elements by inkjet spotting dyes on an array of micropillars (Figure 2). Inkjet spotters are broadly used for integrating biological reagents to diagnostic devices and can easily dispense aqueous solutions at high-throughput, with a lateral positioning accuracy in the micrometer range, and with droplets of picoliters in volume.

Spread of the spotted ink on planar surfaces limits the minimum separation between adjacent code elements, and consequently the maximum spatial density of an optical code that can be written. Spotting the ink inside depressed microstructures, for example, microwells, circumvents this spreading; however, we observed that the dye accumulated at the corners inside the microwells upon drying, and led to nonuniform code elements. Alternatively, when the ink was spotted on top of micropillars, i.e. raised microstructures, contact line pinning at the periphery of the top surface prevented the ink from spreading, and yielded well-defined circular code elements. PEG included in the ink as a drying agent suppressed the coffee ring effect, and further improved the optical quality of the codes (Figure 2a). We used micropillars with a diameter of 150 μm, which were able to hold a single droplet of ink (~400 pL). The pillars were spaced at least 25 μm apart to tolerate possible failures in pinning of the ink. These settings translated into a code having up to 32 elements per mm² and a patterning error rate of 0.2%. Such low error rates can be corrected by including additional code elements and using algorithms for error-correction such as the Reed-Solomon algorithm.

Code elements were arranged to store binary data or human-readable alphanumeric characters (Figure 2b). A security printing strategy can also be utilized to raise the manufacturing barrier against counterfeiters. This strategy can use materials for example with special spectral properties such as upconversion nanoparticles, lanthanide-organic frameworks, phase-change nanoparticles, or solid-state tunable-fluorescence hetero-rotaxanes.

Micropillars are easily fabricated in a Si substrate simultaneously with microlithic structures using conventional lithography and etching techniques. A 2-mask fabrication process can produce pillars of intermediate height to allow interaction between the code elements and a liquid filling the microlithic structures (Figure 2c). Writing a code can in principle be done during the step used for integrating reagents into RDTs.

**Dynamic Optical Security Codes Inside Microchannels.** Reuse of single-use medical products after sterilization and reprocessing is surprisingly very common in hospitals worldwide and presents ethical and hygienic issues. In a similar way, counterfeiters may scavenge, clean, repackage and sell used RDTs again. An optical security code as demonstrated above is static and cannot readily indicate if a device has already been used. However, a dynamic code that is deleted with the sample may warn a user against the reuse of a device would the code not be present.

We implemented dynamic codes by depositing dyes onto micropillars placed inside Si microchannels (Figure 3a and b).

![Figure 3](image-url)

The code can be placed in a flow path parallel to the test channel or downstream to the test region to avoid potential cross-reactivity of the code with the test. The native oxide of the Si layer and the hydrophilic DFR sealing layer make the microchannel capillary active. It took less than 10 s for an aqueous solution to fill the microchannel spontaneously and erase the code by dissolving the dye in the example displayed in Figure 3c. This code only occupies 4 mm² of area and necessitates as little as 110 nL of sample to be completely erased. Such dynamic codes have a slightly lower spatial density than static codes due to the extra space required by the walls used to guide the liquid across each code element. The code in Figure 3c specifically includes 20-μm-wide walls that are 15 μm wide.
away from the pillars, which results in a density of 25 code elements per mm².

Exploiting the interaction between a liquid sample and code elements brings many options for improving security of the devices. Water-soluble and insoluble code elements can be combined to create codes with permanent and erasable code elements that yield a different code pattern after the flow of sample. An invisible and therefore copy-proof code can appear transiently after a reaction with the liquid sample and fade away to prevent reuse.50 Test results can also be encoded in dynamic codes.51

**Partial Deletion of Dynamic Optical Security Codes on Nitrocellulose Membranes.** The majority of RDTs currently used worldwide employ the principle of “lateral flow assays” and a nitrocellulose substrate.6 These tests are particularly easy to counterfeit. Taking this into consideration, we developed dynamic optical codes for nitrocellulose, which can be partially deleted as an additional feature. Such codes not only enable the detection of used tests, but also increase the amount of information that can be stored. Figure 4a and Video S-1 show the transformation of an 8-color code on nitrocellulose within 5 min as an aqueous solution wicks the membrane. This duration is well within the typical time required by biochemical assays.

We found that code elements patterned using inks containing long polymers such as PEG-3000 are retained during migration of liquids on the nitrocellulose. Labile code elements were produced by replacing the PEG with glycerol. Using additives instead of water-soluble and nonsoluble dyes is simpler for implementing partially deleted codes because (1) the same dyes can be used for both types of code elements, which makes their optical properties indistinguishable, (2) both inks have similar viscosity and surface tension, and produce similar patterns, and (3) aqueous solutions are easier to dispense with inkjet spotting than organic solvent based solutions.

It was possible to produce codes on a nitrocellulose membrane with as many as 100 code elements per mm² (100 μm diameter, 100 μm pitch, Figure S-1). Such codes are in line with the optical resolution of commercially available optical readers for POCD devices.25,53 We also simplified some codes to make them readable with smartphones. Specifically, a smartphone camera equipped with a low-cost clip-on macro lens giving a 2× magnification was able to resolve optical codes composed of 500-μm-diameter elements spaced by 500 μm (4 code elements per mm², Figure 4b).

**Reading and Decoding Optical Security Codes.** Optical security codes on a reflective surface such as Si or white support such as a nitrocellulose membrane have good contrast and can easily be captured with a smartphone camera. We developed a software for scanning optical codes, decoding them, and verifying the authenticity of tests. The optical security codes were detected using a method based on template matching. Briefly, asymmetric alignment marks were searched within the scan area (red rectangle seen on the phone display in Figure 4b) to detect the position, size, and rotation of the code. The alignment marks also provided reference points for calibration of the colors to account for variations with ambient light. The value of each code element was subsequently extracted using its position and color. This process took around 50 ms on average, allowing for a hand-held operation.

The capacity of the codes might be limited by the area available on the device. An efficient way of using compact optical codes is to couple the code to additional information on a package. Such information can be stored in a high-capacity QR-code and relate to the type of test, its expiration date, expected geographical area of use, etc. Here, the QR-code contains the address of a server, a shipment identifier, and encrypted data containing the expected value of the optical security code (Figure 4c). Once the QR-code is scanned using a smartphone, the phone connects to the server to receive a decryption key, which is used to decipher the encrypted part of the QR-code. The server also sends information about the test specifications and operating instructions. A test is validated if the decrypted security code from the QR-code matches the read optical security code. This strategy ensures that a test belongs to the intended package, hence essential information such as the type of the test and the expiration date is trustworthy. The server can supply information related to a shipment so that authentication of a first test can enable authentication of additional tests without further need for connectivity.

**Information Capacity of Optical Security Codes.** Figure 5a recapitulates different types of codes presented in this work.
Static codes do not evolve during a test whereas dynamic codes interact with a sample and change. This change can be a partial or complete deletion of the code. Moreover, code elements may be deleted in multiple steps to add further complexity to the codes. When using a single color for static codes, 1 code element corresponds to 1 bit of information (Figure 5b, solid black line). Incorporating $N_{\text{color}}$ colors to the code elements increases the capacity of the code element by $\log_2(N_{\text{color}})$ (for 8 colors see Figure 5b, solid blue line). Dynamic codes with 1-step complete deletion have the same capacity as the static codes.

Dynamic codes that are partially deleted in one step have 1.585 times more capacity compared to static codes with the same number of code elements (Figure 5b, dashed black line, eq 1). Dynamic codes with multiple colors gain extra capacity similarly to static codes (Figure 5b, dashed blue line). The dynamic code on the nitrocellulose membrane in Figure 4a stores 152 bits of information (at least $10^{45}$ combinations) in 32 code elements. The WHO estimated that 314 million RDTs for malaria were used in 2014.54 A dynamic code having as few as 24 single-color elements and 1 partial deletion step can easily provide a specific code for 1000 times this number of RDTs.

Last example in Figure 5a illustrates a dynamic code that is deleted in 4 steps, where one row of the code is affected at each deletion step. In general, the order of deleted rows can change, multiple rows can be deleted simultaneously, or some rows may remain unchanged. These possibilities add a time-dimension to the transformation of the optical security codes. Different combinations to delete a code add 7.2 extra bits of information with 4 deletion steps, and 20.1 extra bits with 8 deletion steps (Figure 5b, dashed lines, eq 2). An implementation for creating dynamic codes with multiple deletion steps is introduced below.

**Implementation of Multiple Deletion Steps.** A microfluidic network analogous to the crossbar switches in electronics can be implemented using a 3D architecture, where a top microfluidic layer, which contains chambers for code elements and an array of routing nodes, is connected to a bottom microfluidic layer through vias (Figure 6a). Each routing node has a capillary stop valve, therefore a liquid cannot enter the node unless it is activated by spotting a

**Figure 5.** Different types of optical security codes and their corresponding information capacity. (a) Illustration of the types of optical security codes included in this work. The brackets on the multistep partial deletion example indicate the row of the code that is partially deleted at a particular step. (b) The information capacity of codes shown in panel (a), plotted as a function of the number of code elements, colors, and deletion steps for removing some of the elements. Black lines indicate codes having 1 color and that are static (solid line) or have from 1 to 8 partial deletion steps (dashed and dotted lines). The capacity of codes including 8 colors are indicated using blue lines.

**Figure 6.** Implementation of an optical code that can be deleted in 4 steps by a liquid in a 3D microfluidic architecture. (a) 3D representation of the microfluidic flow path showing the top and bottom layers and the connecting vias. (b) The top view of the 3D architecture detailing the microfluidic design and its components. The top microfluidic layer contains chambers with the code elements, an array of routing nodes, and 1 inlet and 4 possible outlet microchannels for the liquid. The bottom microfluidic layer contains flow diodes. Arrows indicate the flow direction of the liquid during 2 consecutive deletion steps (first step, with black, and the second with orange arrows). The inset details components of the node. (c) Microscopy images showing the deletion of code elements by water passing sequentially through activated routing nodes. This architecture is microfabricated in Si. Blue rectangles in the first frame indicate the nodes that are activated by spotting black dye inside them. (d) The gain in information capacity when using multistep codes as a function of the number of deletion steps, $b$, compared to static codes having the
same amount of code elements. (e) The factor of lost chip area ($A_{\text{chip}} = 200 \times 200 \mu m^2$, $A_{\text{node}} = 400 \times 500 \mu m^2$) and (f) the gain in code writing speed ($t_{\text{spot}} = 1$ s) when using multistep codes compared to static codes containing the same amount of information. $n$ is the number of code elements, and $b = n$ shows the upper boundary where each code element can be deleted individually.

wetting agent next to its valve. If activated, the liquid can pass through the node and proceed to the downstream chamber where it can delete code elements. The flow diodes at the bottom microfluidic layer force the liquid to travel only to downstream chambers. Activation of multiple nodes set the sequence of the chambers to be filled (Figure 6b). Figure 6c and Video S-2 show a liquid filling such an architecture and erasing the code in 4 steps. In this example, the microchannels are 100 μm wide and 20 μm deep. The width of the capillary valves is 10 μm and the constrictions of the flow diodes are 25 μm. The vias have a diameter of 50 μm and a length of 360 μm. The dimensions of the spotting areas for node activation are 200 × 100 μm² and can easily be targeted with the inkjet spotter.

Multiple-step deletion of codes using this implementation has interesting outcomes. First, extra information is stored in how the code evolves, which augments the capacity of the codes especially of those with few elements (Figure 6d, eq 2). Second, this extra information can be extracted only by observing the transformation of the code during the use of a test. Therefore, the array of nodes can be completely concealed from the user and/or transparent reagents can be used for activating the nodes. This adds a covert security feature to the optical codes and complicates copying attempts by adversaries. The array of nodes uses additional chip area but this penalty diminishes for codes having high-capacity (Figure 6e, eq 6). Additionally, the mean time to write such codes decreases because spotting reagents on the array of nodes gives more combinations than when the same number of spots would be used in binary coding (Figure 6f, eq 5).

## CONCLUSION

Counterfeiting is a huge activity, worth hundreds of billions of dollars and spanning nearly all sectors of industry. It is much more widespread than known to the public and is getting progressively worse. Counterfeiters are very creative and determined, whereas end-users are generally not able to discriminate fake products. This situation can have particularly dramatic consequences when counterfeit diagnostic devices are used. For this reason, it may be strategic for the large communities working on many new diagnostic devices and biosensors to consider adding security features to their next generation of analytical devices.

## ASSOCIATED CONTENT

### Supporting Information

The Supporting Information is available free of charge on the ACS Publications website at DOI: 10.1021/acs.analchem.8b00826.

Characterization of the printing resolution of the inkjet spotter with the amaranth ink on the nitrocellulose membrane (PDF)

Video of an 8-color dynamic code on the nitrocellulose membrane that is partially deleted in a single step (AVI)

Video of a liquid filling the 3D architecture and deleting the code in 4 steps (AVI)

## AUTHOR INFORMATION

### Corresponding Authors

*E-mail: ogo@zurich.ibm.com. Tel: +41-44-724 8935.
*E-mail: emdq@zurich.ibm.com. Tel: +41-44-724 8283.

**ORCID**

Emmanuel Delamarche: 0000-0002-8753-8895

**Notes**

The authors declare no competing financial interest.

### ACKNOWLEDGMENTS

We thank Yuksel Temiz and Ute Drechsler for their help in chip fabrication, Diana Davila Pineda for the SEM images, Andreas Kind for providing insight on counterfeiting and security solutions, and Walter Riess for his continuous support. We acknowledge partial funding from the IBM Research Frontiers Institute.

### REFERENCES


(51) Yang, M.; Zhang, W.; Zheng, W.; Cao, F.; Jiang, X. Lab Chip 2017, 17, 3874−3882.


