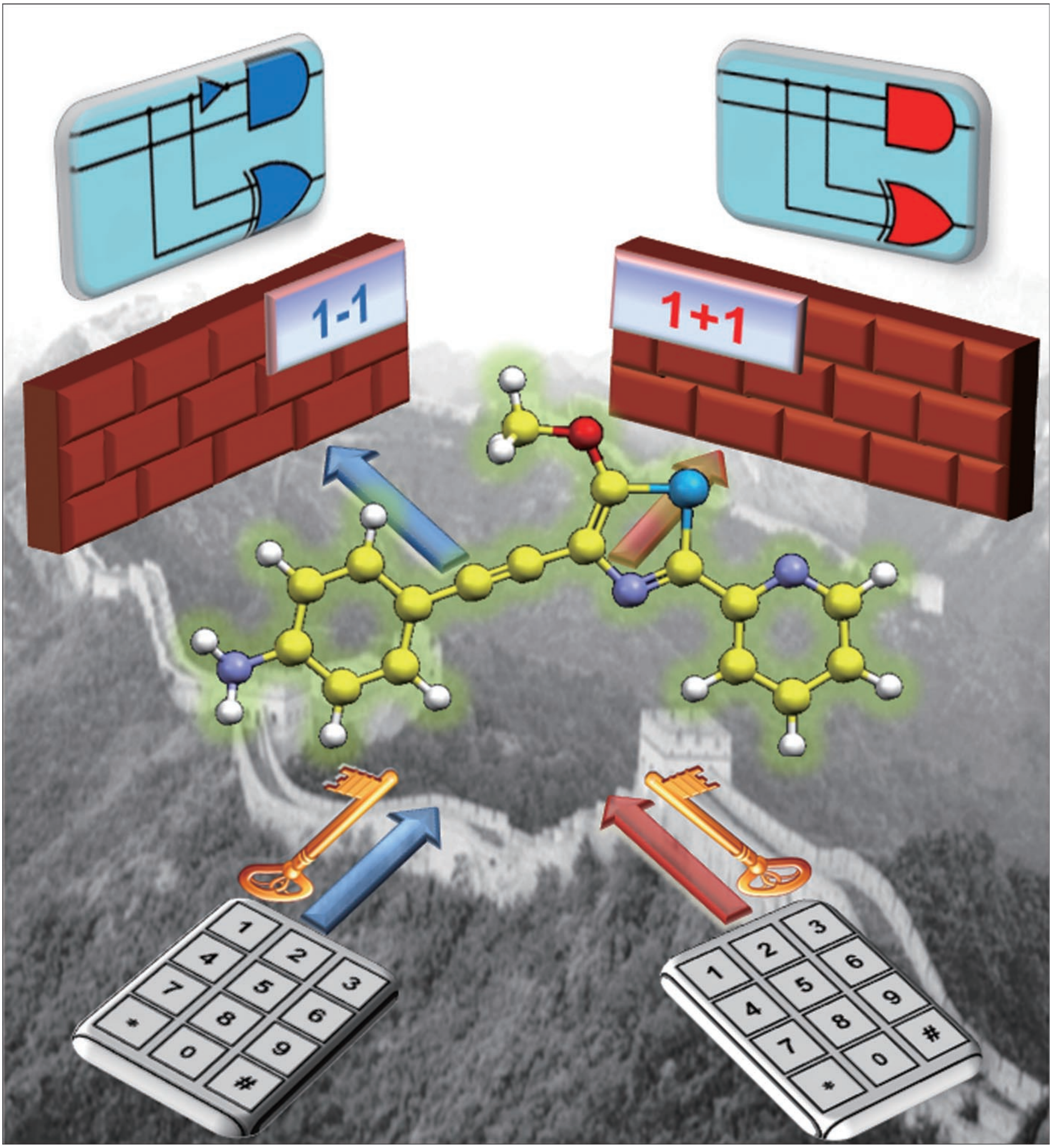
CHEMISTRY
A EUROPEAN JOURNAL

DOI: 10.1002/chem.200800576

A Fluorescent-Switch-Based Computing Platform in Defending Information Risk

Wei Sun, Can Zhou, Chun-Hu Xu, Chen-Jie Fang, Chao Zhang, Zhan-Xian Li, and Chun-Hua Yan*[a]



Abstract: A molecular computing platform to defend against illegal information theft and invasion is obtained by the rational control of chemical reaction sequences in a newly prepared multiswitchable fluorophore 2-(4-aminophenylethylyl)-5-methoxy-2-(2-pyridyl)thiazole. Some of the fluorescent states with distinct recognition features are only activated through input-sequence-sensitive conversions. Chemically encoded user identity information can then be transmitted from a sequential logic unit to a combinational logic circuit, and hence, result in user-specific digital functionalities. The user's password entry is authorized prior to each computing step to check not only the user's identity, but also to reconfigure the molecular platform from the standby state to the corresponding operational state. Illegal accesses to the molecular computing platform are unable to activate the operation of the trusted users due to the incorrect activation processes, thereby ensuring the information is secured against information invasions.

Keywords: fluorescent probes • logic gates • molecular devices • protonation • supramolecular chemistry

Introduction

It has been demonstrated that in recent years nano or subnanoscale computing devices are being constructed through a bottom-up approach.[1] In particular, the development of molecular devices has inspired chemists to use small molecules as versatile building blocks for nanoscale devices for a wide range of digital functionalities from data storage,[2] numerical processing,[3] and quiz games[4] to password entries.[5] However, compared with electronic computing devices, no report of molecular devices capable of providing user-specific computing functionalities has been published to date. This may be due to the difficulties in transferring identity information from the authentication unit to the execution unit at the molecular level. The open and flexible working mode of molecular devices serves as a double-edged sword, offering ease in use but poor security levels in practical applications, especially when the same computing functionalities can be accessed by both the trusted users and the invaders. From a viewpoint of potential applications it is necessary to strengthen the security of molecular devices.

One strategy to elevate the security level in modern computing devices, such as laptop PCs, cellular phones, and automated teller machines, is to distinguish users' identities and then endow them with distinct digital functionalities.[6] For instance, the authentication-prior-to-execution strategy has been widely used as the login step of personal computers and network servers, in which the administrator and the guest users access distinct databases and functionalities according to their passwords. If this strategy is implemented into the molecular computing devices, the subnanoscale platform will be equipped with a hardware defense against information invasion during its execution and communication processes.

Herein, we present a prototypical molecular platform to ensure information security against illegal invasion. All of the digital functionalities are executed within a newly prepared fluorescent switch, 2-(4-aminophenylethylyl)-5-methoxy-2-(2-pyridyl)thiazole (MPTEA), through simple chemical reactions, such as acylation, protonation, and coordination. Some fluorescent derivatives of MPTEA with distinct binding features are activated only after the in situ chemical conversion from neutral MPTEA. From a viewpoint of information security, the transformation among various fluorescent states of MPTEA can be encoded with the authentication-prior-to-execution strategy. When operating this molecular system one needs to present credentials to the platform through the accurate chemical/irradiation encoded password entry, which activates the specific fluorescent state of MPTEA, and then the user is allowed to access the specific digital functionality depending on the activated binding feature of the fluorescent state. Based on the authentication-prior-to-execution strategy, the security feature of current chemically driven molecular platforms is achieved through three interrelating steps: 1) password authentication for the user identity information, 2) authentication-directed reconfiguration of processing units for the user-specific binary algebra functionality, and 3) encrypted output interface for optical communication and data storage. Two users operating distinct logic computing functionalities, including binary algebra and secured data communication and storage, can be then distinguished by the molecular platform.

Results and Discussion

Design: The key challenge in implementing a computing device with security features is how to recognize the user's identity information by a sequential logic circuit, and utilize it to reconfigure the data processing unit with specific functionality. It is particularly difficult in the molecular logic device (Figure 1a), in which the input and output signals of

[a] W. Sun, C. Zhou, C.-H. Xu, Dr. C.-J. Fang, C. Zhang, Dr. Z.-X. Li, Prof. Dr. C.-H. Yan
Beijing National Laboratory for Molecular Sciences
State Key Lab of Rare Earth Materials Chemistry
and Applications & PKU-HKU Joint Lab
in Rare Earth Materials and Bioinorganic Chemistry
Peking University
Beijing 100871 (China)
Fax: (+86) 10-6275-4179
E-mail: yan@pku.edu.cn

Supporting information for this article is available on the WWW under http://www.chemeurj.org/ or from the author.

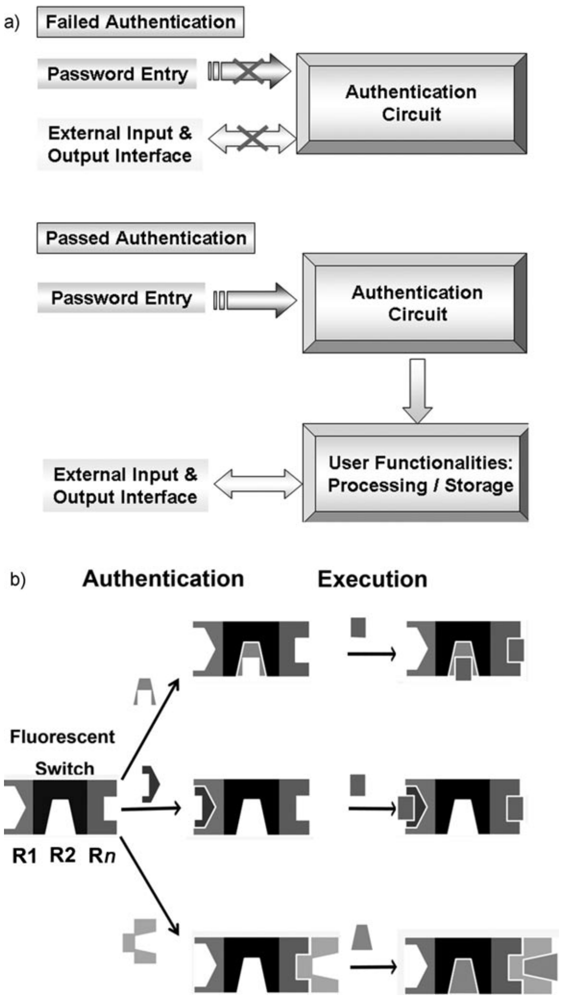


Figure 1. Operation principle (a) and design strategy (b) for molecular devices with the authentication-prior-to-execution strategy. R1, R2, and R*n* represent different receptor sites of the fluorescent switch. Different symbols above the arrows represent various chemical or photo-optical input signals.

the logic circuit are heterogeneous.[7] From a supramolecular chemistry viewpoint, password authentication for user identity is based on the response to both the sequence and the nature of the input signals in chemically driven logic systems,[5a] whereas data processing, such as binary algebra,[3] is based on recognition between the fluorescent switch and specific input signals. If the recognition is only activated after an input-sequence-sensitive conversion from the initial form, the fluorescent switch is thus capable of transferring the user's identity information to the data processing unit. Different binding features between the initial fluorescent switch and the activated fluorescent form ensure that the logic functionalities are achieved only after activation, which reveals that the logic functionalities are secure to illegal access. The fluorescent switch then acts as both the information carrier and the information executor, enabling the authentication-prior-to-execution strategy within a molecular device. If there is more than one reaction pathway to activate the receptor sites, the molecular device will be capable of distinguishing multiple users (Figure 1b).

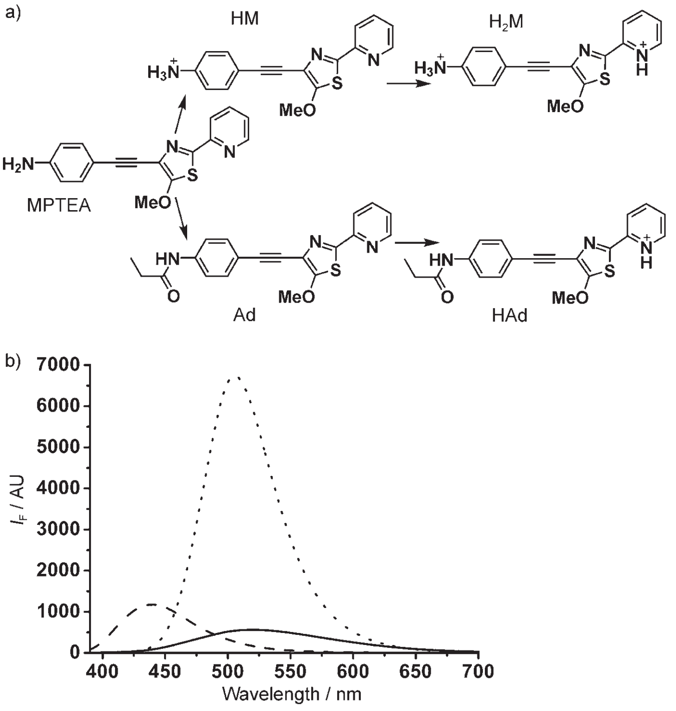
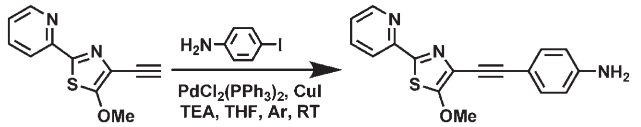


Figure 2. Fluorescence of different MPTEA binding states. a) The activation pathways for various MPTEA binding states: MPTEA (——), Ad and HM (– – –), HAd and H_2M (-----). b) Fluorescent spectra of the corresponding states. Concentration of each species is 0.04 mM, and emission spectra are recorded with the excitation at 350 nm.



Scheme 1. Reaction route of MPTEA.

According to the design principle above, a multiswitchable fluorescent switch, 2-(4-aminophenylethylyl)-5-methoxy-2-(2-pyridyl)thiazole (MPTEA), was designed to be attached with multiple receptor sites, including an amino group and a pyridine ring (Figure 2) and was synthesized following a modified Sonogashira coupling procedure (Scheme 1).[8] Neutral MPTEA exhibits a broad emission band centered at 515 nm. The fluorescent states can be modulated by different chemical inputs. Both the amino group and the pyridine ring can bind with a proton, however, the binding constants are different (the pK_a value in water is 4.59 for aniline,[9] and 1.6 for 5-methoxy-2-(2-pyridiyl)thiazole (MPT)[10]). Therefore, MPTEA can be protonated stepwise. The introduction of a small amount of proton triggers the first protonation at the amino group and produces monoprotonated MPTEA (HM) with an emission band centered at 435 nm. Further protonation at the pyridine ring converts HM to the diprotonated MPTEA (H_2M) with enhanced emission intensity at 500 nm. The existence of an amino group also provides a binding site for acylation. When treated with propionyl chloride (PPC), the amino group in MPTEA is converted into the corresponding amide form (Ad), along with a blue emission band centered at 435 nm.

Addition of proton to a solution of Ad protonates the pyridine ring to afford HAd, with similar spectral properties to that of H_2M. Analogous to those of the parent compound MPT,[10] the fluorescent properties of MPTEA originate from intramolecular charge-transfer (ICT) processes from electron donors, such as amino and methoxy groups, to an electron accepting pyridine ring. Either protonation or acylation at the amino group decreases the electron-donating ability of the nitrogen atom, which hypsochromically shifts the emission band. Protonation at the pyridine ring increases its electron-withdrawing ability and enhances ICT efficiency with a bathochromic shift of the emission band. Moreover, both the amino group and the pyridine ring can also bind with a paramagnetic cupric ion to form nonfluorescent complexes.[8]

User authentication: As the first step toward hardware-based protection, authentication for two trusted users are encoded within the input-sequence-sensitive in situ transformation among distinct fluorescent states, only allowing users holding correct password entries to access the pre-programmed digital functionalities. MPTEA in acetonitrile (0.02 mM) containing *n*-butylamine (0.1 M) is set as the standby state of the secured platform. Similar to a previous report, a four-digit password is entered through a keypad,[5] on which digital numbers represent various chemical and irradiation input signals. For example, buttons labeled 1, 2, 3, and 4 in the keypad represent irradiation at 350 nm for 2 min, *n*-butylamine (0.1 M), trifluoroacetic acid (TFA, 0.1 M), and propionyl chloride (PPC, 1 mM)/$CuCl_2$ (0.06 mM), respectively. The other buttons represent the introduction of a large amount quenchers (Figure 3a). When a single button is pressed, the corresponding chemical or irradiation input is introduced into the quartz cell to react with the fluorescent substrate. Each individual button can be pressed repeatedly, producing 10^4 possible input sequences for the 4-digit password. Fluorescent signals during chemical conversions are utilized to distinguish different users. However, if the fluorescent intensity during the authentication process is not higher than the noise of the detector, the fluorescent signal will be denoted as dark noise and the value is not recorded.

The transformation from MPTEA to H_2M is accomplished by consecutive addition of two portions of TFA solutions, and visualized with excitation of 350 nm light. Hence, input sequence 1331 is the only password entry to pass the authorization for user 1, in which the emission intensity of

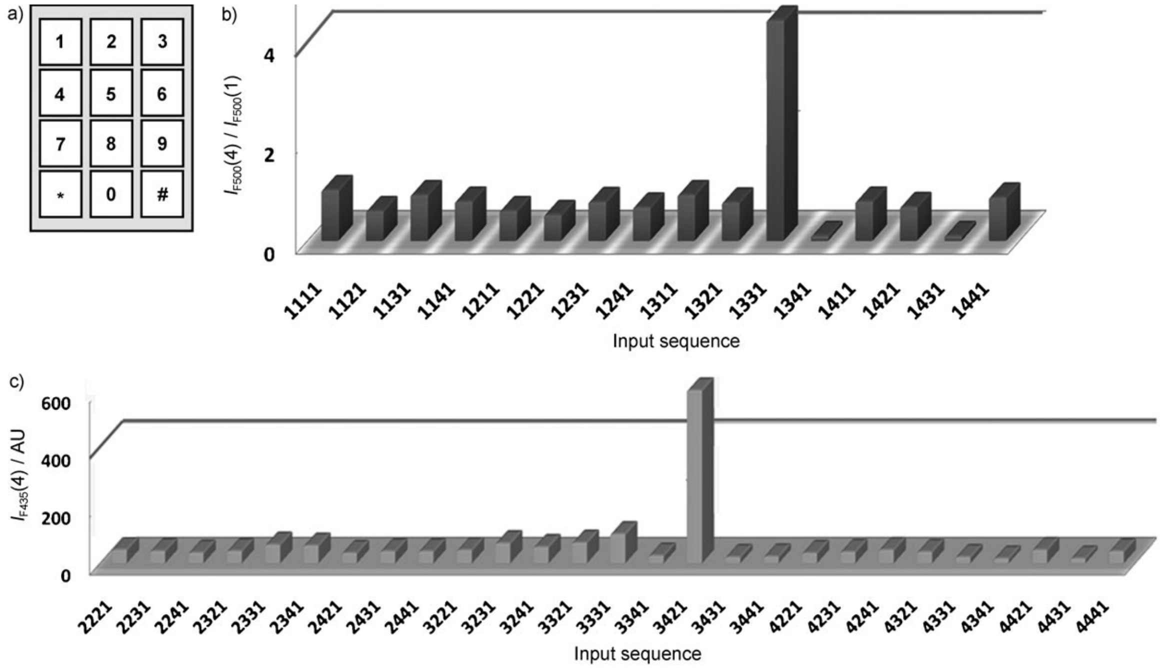


Figure 3. Fluorescent signals for the authentication processes. a) Buttons 1, 2, 3, and 4 on the keypad represent irradiation at 350 nm for 2 min, *n*-butylamine (0.1 M), TFA (0.1 M), and PPC (1 mM)/$CuCl_2$ (0.06 mM), respectively. Other buttons represent an excess of quenchers. The initial solution is MPTEA (0.02 mM) containing *n*-butylamine (0.1 M) in acetonitrile. b) Authentication signals of user 1. The output channel is selected as the ratio of fluorescent intensity at the fourth step to that at the first step recorded at 500 nm ($I_{F500}(4)/I_{F500}(1)$). c) Authentication signals of user 2. The output channel is selected as the fluorescent intensity at the fourth step recorded at 435 nm ($I_{F435}(4)$). The solid line in Figure 3b and c represents the threshold value for the authentication of each specific user.

the final step must be four times higher than that of the first step at 500 nm wavelength. The first and the fourth input step of button 1 produce the fluorescent signal for the evaluation of the password. While the second input step of button 3 neutralizes the initial *n*-butylamine, and the third input step of button 3 triggers the protonation of MPTEA.

The uniqueness of password 1331 for user 1 is validated as follows: For any 4-digit number strings containing buttons represented by quenchers (i.e., button 5), the final solution state is nonfluorescent, and thus the authorization fails. As for user 1, the requirement to pass authorization is that the emission intensity of final step is four times higher than that of the first step at 500 nm. The first and fourth digit of the password entry has to hold button 1 (irradiation at 350 nm) to achieve fluorescent output signals; otherwise only background noise exists and no intensity value is recorded according to the system settings. Thus, only 16 possible interfering states remain out of 10^4 original possibilities. As shown in Figure 3b, only one number string, 1331, produces the correct authentication result. Notably, for a keypad in Figure 3a, an *n*-digit password entry without identical terms will afford distinct interfering items equal to the factorial of *n* (*n*!), less than those entries with identical terms, which is equal to 10^n.

Similarly, password entry 3421 produces Ad as the final state with a strong blue emission band centered at 435 nm, which identifies the authorization code for user 2, in which emission intensity of the final step must be over a threshold of 400 AU in intensity. The first input step of button 3 introduces TFA to neutralize the initial *n*-butylamine. The second input step of button 4 introduces PPC to convert MPTEA to the Ad form, and the cupric ions also simultaneously introduced by button 4 bind with Ad to give the nonfluorescent form. The introduction of *n*-butylamine, as the third input step of button 2, removes cupric ions from the nonfluorescent complex, and releases Ad. While the last input step of button 1 triggers the optical signal for the evaluation of the password.

The uniqueness of 3421 for user 2 can be discussed in an analogous way to that given above for user 1: If the 4-digit number input contains buttons represented by quenchers (i.e., button 5) the final solution state is nonfluorescent, and thus authorization fails. As for user 2, sufficiently high emission intensity is the requirement to pass authorization in the final step. Therefore, the fourth digit of the password has to be button 1 (irradiation at 350 nm) to achieve a fluorescent output signal. Thus, the original 10^4 possibilities are reduced to 64 possibilities. Notably, excess *n*-butylamine quenches PPC and in turn prohibits the conversion of MPTEA to Ad, so TFA has to be introduced before PPC to neutralize *n*-butylamine, which means that button 3 must be pressed before button 2. However, *n*-butylamine can also bind with cupric ions, which are released, by pressing button 2, from the nonfluorescent complex to liberate the fluorophore Ad. Therefore, button 2 has to be pressed after button 4. Thus, the transformation from MPTEA to the free Ad form is achieved by at least a three-step sequence of pressing chemically encoded buttons, restricting only a step irradiation pulse to the four-digit password entry. Only 27 possible interfering states then remain out of the original 10^4 possibilities. As shown in Figure 3c, sequence 3421 is the unique one to allow the authorization of user 2.

Binary algebra: Binary algebra functionality is activated after the authorization step, in which two sets of input signals are composed of the proper combination of chemical and irradiation signals. Input set 1 is selected as the introduction of 0.1 M *n*-butylamine plus the irradiation at 350 nm for 2 min (I1) and the irradiation at 410 nm for 2 min (I2), whereas input set 2 is selected as two equal portions of 0.8 M TFA (I3 and I4), and the operation of input set 2 is under the excitation at 350 nm. The corresponding output channels are set as the changes of fluorescent signals at various wavelengths in response to the input sets. The output channels in response to input set 1, denoted as output set 1, are selected as the emission intensity at 525 nm (O1), and the emission intensity ratio at 500 nm to that at 525 nm (O2). The logic state 0 is defined as the signal intensity below 150 for O1 and below 1 for O2 in output set 1. The output channels in response to input set 2, denoted as output set 2, are selected as the emission intensities at 485 (O3) and 520 nm (O4). The logic state 0 in output set 2 is defined as the signal intensity above 150 for O1 (negative logic[11]) and below 150 for O2, respectively.

When user 1 logs into the molecular platform, his password entry 1331 converts the molecular platform from the standby state, namely, MPTEA, to the operational state, namely, H_2M. User 1 is then endowed with half-subtractor functionality when input set 1 is applied. As shown in Figure 4a, fluorescent signals at both channels are below the threshold value (i.e., O1 = O2 = 0) when no input signal is introduced (i.e., I1 = I2 = 0) due to the absence of the excitation source. When I1 is present alone (i.e., I1 = 1, I2 = 0), the introduced *n*-butylamine neutralizes the proton in H_2M to generate neutral MPTEA. The excitation at 350 nm of I1 also triggers a characteristic emission band of neutral MPTEA, which is centered at 515 nm with the emission intensity ratio of the emissions at 500 and 525 nm equal to 1 (i.e., O1 = 1, O2 = 0). When I2 is present alone (i.e., I1 = 0, I2 = 1), the excitation at 410 nm of I2 triggers a characteristic emission band of the diprotonated form H_2M, which is centered at 500 nm with the emission intensity ratio of the emissions at 500 and 525 nm larger than 1 (i.e., O1 = 1, O2 = 1). Simultaneous addition of I1 and I2 (i.e., I1 = I2 = 1) also produces MPTEA by the introduction of *n*-butylamine in I1, but the subsequently introduced excitation at 410 nm of I2 fails to excite the emission band of MPTEA (i.e., O1 = O2 = 0).[3e] An XOR gate is then constructed at O1 and an INHIBIT gate is constructed at O2. Thus, a half-subtractor is accessible for user 1 when input set 1 and the corresponding output set are employed. However, the same input and output sets cannot retain the subtraction functionality for either unauthorized users or user 2. As shown in Figure 4 and Table 1, input set 1 only produces PASS 0 gates at both

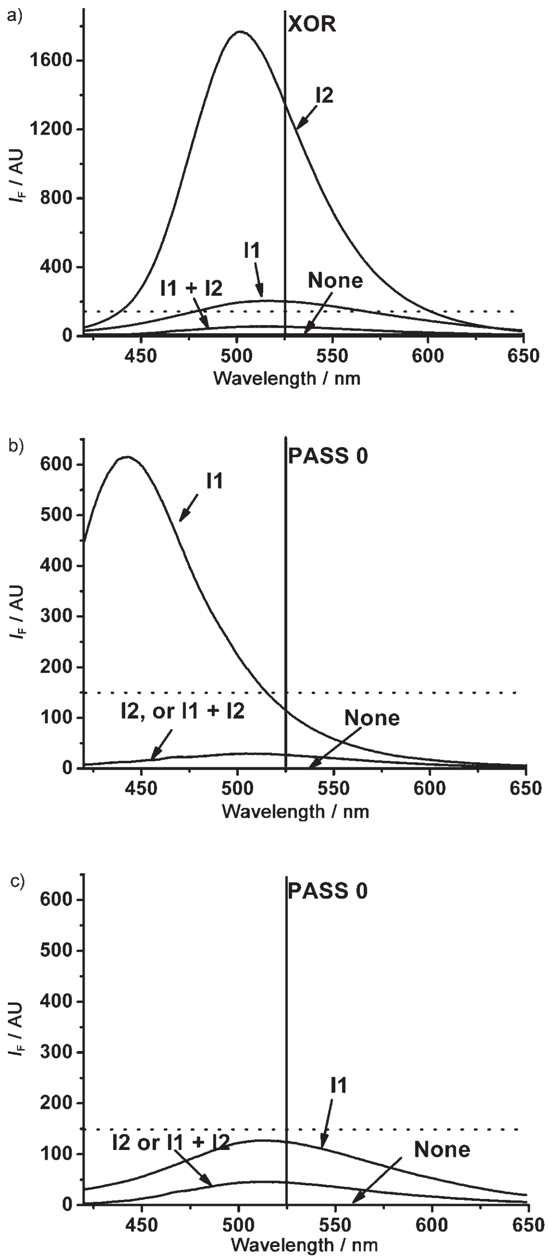


Figure 4. User-specific half-subtractor functionality under input set 1. a) Fluorescence spectra of half-subtractor for user 1. b) Fluorescence spectra for user 2. c) Fluorescence spectra for the unauthorized user. I1: *n*-butylamine (0.1 M) plus an excitation pulse at 350 nm for 2 min. I2: excitation pulse at 410 nm for 2 min. O1: emission intensity at 525 nm. O2: emission intensity ratio at 500 nm to that at 525 nm. The logic state 0 is denoted as a signal intensity below 150 in O1 and below 1 in O2. The dotted line represents the threshold. Table 1 gives the truth table for the different logic behaviors shown in a), b), and c).

channels of output set 1 for the unauthorized users. Whereas for user 2, input set 1 produces PASS 0 gate at O1 and INHIBIT gate at O2. Thus user 1 is the only one allowed to access the half-subtractor.

As for user 2, the introduction of input set 2 produces the half-adder functionality (Figure 5a). When user 2 logs into the molecular platform, password entry 3421 converts the molecular platform from the standby state to the operational state, namely, Ad with *n*-butylamine coordinated to cupric ions. Thus, input set 2 switches the protonation states of Ad. When no input signal is introduced, the excitation at 350 nm results in a characteristic emission band of Ad with a high fluorescent intensity at 485 nm (i.e., O3 = O4 = 0). The introduction of one portion of TFA (I1 = 1, I2 = 0, or I1 = 0, I2 = 1) neutralizes the initial *n*-butylamine, but fails to bind with Ad due to competition from cupric ions, resulting in low output signal at both channels (i.e., O3 = 1, O4 = 0). The consecutive introduction of two portions of TFA (i.e., I3 = I4 = 1) adds excess protons into the solution, which converts Ad to the protonated HAd form even in the presence of cupric ions in the solution. The excitation at 350 nm triggers the characteristic emission band of HAd with a high fluorescent intensity at both channels (i.e., O3 = 0, O4 = 1). An XOR gate is constructed at O3, while an AND gate is constructed at O4. Thus, a half-adder is accessible for user 2 when input set 2 and the corresponding output set are built up. In a similar manner to the cases in the half-subtractor, user 1 and the unauthorized users cannot access the half-adder functionality even applied with input set 2. As shown in Figure 5 and Table 2, input set 2 only produces PASS 0 gates at O3 and PASS 1 gate at O4 for both the unauthorized users and user 1. Hence, the security of the half-adder for user 2 is guaranteed.

The reason that the arithmetic functionality is not retained when no valid user presents credentials to the platform lies in the fact that chemically driven logic functions are determined by both the input signals and the initial working conditions. The difference in the binding modes of various initial working conditions induces varied logic expressions at the corresponding output channel. As a further interpretation, the XOR gate in both the half-adder (O3) and the half-subtractor (O1) is taken as an example. To construct an XOR gate, the fluorescent switch undergoes an off–on–off three-state switching processes. Thus, the original nonfluorescent state is turned on when each single input exists, but turned off again when both inputs are present. As for the unauthorized user, user 1, and user 2, the initial working conditions are MPTEA, H_2M, and Ad, respectively. However, only H_2M can respond to both I1 and I2 with changing the emission state at O1, whereas the fluorescence of both MPTEA and Ad cannot be excited by I2, which produces an off state. Thus, input set 1 can produce an XOR gate only for user 1. The situation is

Table 1. Truth table for the different behaviors shown in Figure 4.

Input set 1		User 1		User 2		Unauthorized user	
I1	I2	O1	O2	O1	O2	O1	O2
0	0	0 (low, 10)	0 (low, 1.00)	0 (low, 10)	0 (low, 1.00)	0 (low, 10)	0 (low, 1.00)
1	0	1 (high, 220)	0 (low, 0.95)	0 (low, 100)	1 (high, 1.50)	0 (low, 120)	0 (low, 1.00)
0	1	1 (high, 1330)	1 (high, 1.33)	0 (low, 50)	0 (low, 1.00)	0 (low, 50)	0 (low, 1.00)
1	1	0 (low, 50)	0 (low, 1.00)	0 (low, 50)	0 (low, 1.00)	0 (low, 50)	0 (low, 1.00)

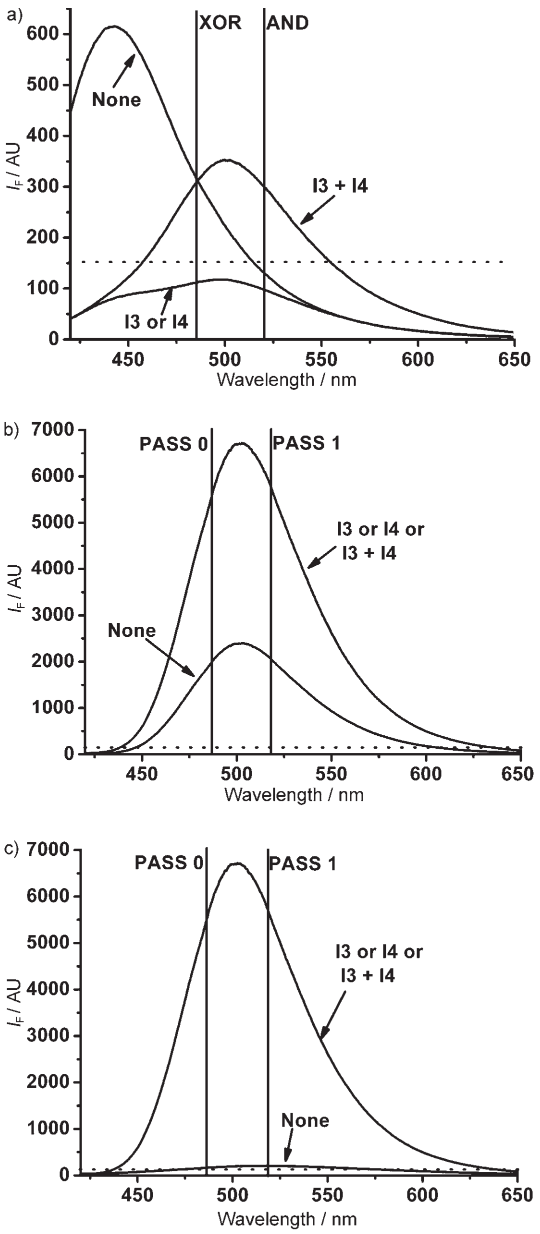


Figure 5. User-specific half-adder functionality under input set 2. a) Fluorescent spectra of half-adder for user 2. b) Fluorescent spectra for user 1. c) Fluorescent spectra for the unauthorized user. I3: TFA (0.8 M). I4: TFA (0.8 M). O3: emission intensity at 485 nm. O4: emission intensity ratio at 520 nm. The fluorescent intensity is recorded under excitation at 350 nm. The logic state 0 is denoted as a signal intensity over 150 in O3 (negative logic[11]) and below 150 in O4. The dotted line represents the threshold. Table 2 gives the truth table for different logic behaviors shown in a), b), and c).

different for the TFA signal in input set 2. Both MPTEA and H_2M exhibit a high emission intensity at 485 nm above the threshold. Introduction of 0.8 M TFA protonates MPTEA to give H_2M, which produces logic state 0 regardless of the input of I3 and I4 at O3. Thus, both input signals of input set 2 fail to switch the logic value of O3. While for Ad, the two-step introduction of TFA turns the protonation states from Ad through cupric-complexed Ad to HAd, and produces the desired off–on–off switching behavior for the XOR gate. The distinct binding modes activated by different sequential conversion pathways provide the desired user-specific algebraic functionalities.

Data encryption: Unprotected optical output signals can be easily wiretapped, making molecular devices vulnerable against illegal listening during data transfer. Digital communication can be protected if keytext is employed to encrypt plain text data into cipher text, which affords distinct binary signals from the unencrypted ones.[12] The same encryption process can be constructed at the current molecular platform by employing chemically encoded input as the keytexts. For each arithmetic step of the half-adder, original fluorescence spectra produced by input set 2 are further switched on or off by keytexts, due to changes in the protonation state. To encrypt optical signals with string encryption cryptology[13] at the present molecular platform, 0.8 M TFA and 0.8 M *n*-butylamine, which can reversibly modulate the protonation equilibrium between Ad and HAd, are added to the solution as chemically encoded keytexts, after the operation by input set 2. The output channel settings remain the same as those in the half-adder. Directly recording the fluorescent signals is not helpful to communicate the correct information. As shown in Table 3, different arithmetic processes can be encrypted to exhibit the same fluorescent output signals with distinct keytext strings. Only when both the encrypted fluorescence output signals and keytext inputs are known can the protected data be decrypted. This requirement is simple for a trusted user holding the keytext entry, but rather difficult for those without any information about keytext. The protection of communication through keytext encryption enables the current molecular platform to exchange information in a secured manner, completing the third step of security policy in the current system.

The secured platform also enables user 2 to store information in a protected manner, so that only the user holding the correct password entry can read the stored information (Figure 6). The readout channel is selected as the emission intensity at 435 nm under excitation at 350 nm. The threshold for logic state 0 is set as 150 AU in intensity. MPTEA performs not only as an authentication unit, but also as a signaling unit. The blue output signal is activated through authorization-triggered conversion from MPTEA to Ad by the password 3421. Tetrathiafulva-

Table 2. Truth table for the different behaviors shown in Figure 5.

Input set 2		User 2		User 1		Unauthorized user	
I3	I4	O3	O4	O3	O4	O3	O4
0	0	0 (low, 300)	0 (low, 140)	0 (low, 1800)	1 (high, 1800)	0 (low, 180)	1 (high, 220)
1	0	1 (high, 100)	0 (low, 90)	0 (low, 5500)	1 (high, 5600)	0 (low, 5500)	1 (high, 5600)
0	1	1 (high, 100)	0 (low, 90)	0 (low, 5500)	1 (high, 5600)	0 (low, 5500)	1 (high, 5600)
1	1	0 (low, 300)	1 (high, 300)	0 (low, 5500)	1 (high, 5600)	0 (low, 5500)	1 (high, 5600)

Table 3. Encrypted output results for a series of half-adder operations of user 2.

Operation[a]	Original output signal[b]	Keytext[c]	Encrypted output signal[d]
0+0, 0+1, 1+1, 0+0, 0+1, 1+1	00-10-01-00-10-01	ANBANN	10-10-10-10-10-01
0+1, 0+1, 1+1, 0+0, 0+1, 1+1	10-10-01-00-10-01	NNBANN	10-10-10-10-10-01
0+1, 1+1, 1+1, 0+0, 0+1, 1+1	10-01-01-00-10-01	NBBANN	10-10-10-10-10-01
0+1, 1+1, 0+0, 0+0, 0+1, 1+1	10-01-00-00-10-01	NBAANN	10-10-10-10-10-01

[a] Operations are recorded as a series of arithmetic steps in response to the input set 2. [b] Original output signal is recorded as the binary output signals at both O3 and O4 channels for each arithmetic step. [c] Keytext is recorded as the input sequence of either A (0.8 M TFA), N (no input), or B (0.8 M *n*-butylamine). [d] Encrypted output signal is recorded as the binary output signals at both O3 and O4 channels for each arithmetic step after encryption. The operations in each row are executed inside a same solution.

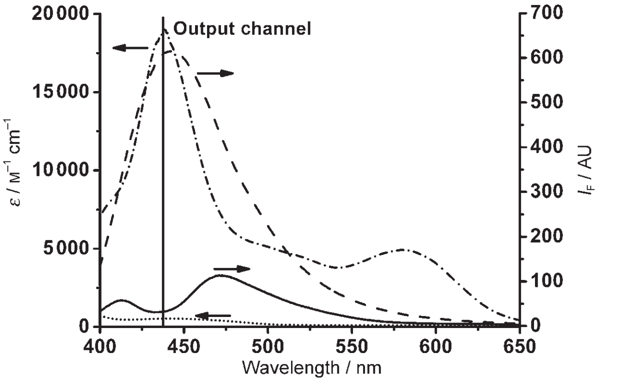


Figure 6. Molecule-based information storage for user 2. The absorption of neutral TTF in the visible region (•••••), the absorption of the cation radical state TTF in the visible region (–•–•), the emission state of the solution when TTF is in the neutral state (-----), and the emission state of the solution when TTF is in the cation radical state (——) are shown. Starting conditions: 0.02 mM MPTEA, 1 mM *n*-butylamine, and 1 mM TTF in acetonitrile. Fluorescence spectra are recorded with excitation at 350 nm.

lene (TTF, 1 mM) is added to the reaction quartz cell to serve as a redox switch for fluorescence signal, owing to its tunable absorption overlap[3c] with the emission of Ad. Write and erase processes are accomplished through reversible redox between neutral and cationic radical TTF states by the introduction of oxidant $NOBF_4$. Cation radical state TTF strongly quenches fluorescence at 435 nm due to the inner filter effect between Ad and TTF^+, while low spectral overlap prevents neutral TTF from quenching the fluorescence at 435 nm. Therefore, attempts to circumvent the authentication step also fail to activate the fluorescent signal channel. A redox-controlled fluorescent switch provides an information storage functionality to the molecular platform, and in situ conversion of signaling unit also brings a built-in security feature to protect the stored information. The protection of stored information is constructed based on the access control, providing an another method besides the steganographic technique in DNA double-strands[13a] and invisible ink technique in self-assembled dendrimers.[13b]

Security policy: The authentication-prior-to-execution strategy applied in electronics may be cracked through a modification chip (modchip) or illegal duplication, and hence, adds an Achilles' heel to the information security policy.[6d] This problem may be solved in molecular devices. In the current molecular platform, each MPTEA molecule contains both an authentication unit and a processing unit. As a result, for each algebraic computing step or data encryption, an MPTEA molecule must undergo in situ conversion before responding to the arithmetic inputs. Thus, any operation related to data processing must be authorized before it is executed. Drastic modifications of the MPTEA structure will break down its original recognition-response correlation and accordingly prohibit expected fluorescence-based digital functionalities. The operational state accessed after authorization also prevents reverse engineering, which is widely used in illegal duplication, due to the fact that the unauthorized user can only investigate the standby state, but knows nothing about the working state for different authorized users.

Reset capacity: From a viewpoint of a potential application, the reset issue in the current chemically driven platform needs to be addressed. The available digital functionalities, including algebraic arithmetic, encrypted communication, and data storage, are based on protonation, coordination, and redox reactions, which have been reported to be resettable by us and other researchers.[3a,c,4c,8] For example, the execution and reset cycles of the binary arithmetic are shown in Figure 7 for both users. Thus, for the same user all of the allowed computing tasks can be reset reversibly. However, the switch of the users' identities is irreversible not only because of the existence of acylation reaction, but also because of the concerns about the information risk upon resetting.[5a] When a new user logs into the system, the identity information of the previous user should be erased irreversibly, thus the latter user cannot know what the previous one has done. When a user logs out of the platform, a large amount of quencher is then introduced to the reaction chamber to deteriorate the fluorescent molecules thoroughly and the solution needs to be refreshed for the next user to login, even if the authentication process is reversible, as in the case of user 1 utilizing protonation equilibrium for authentication.

The operation of the current molecular platform also faces challenges of accumulation of chemical waste due to the consumption of high concentrations of acid and base, which is a common problem for chemically driven logic gates and devices and prevents them from practical use.[5a] In particular, refreshing the initial solution after each authentication attempt will also increase solution consumption. Further integration of the secured platform with cheap paper strips or microfluidic devices may overcome this obstacle and promote the potential fabrication of commercially available molecular logic devices.[14] For example, only nanoliters of solution are required for each logic operation in mi-

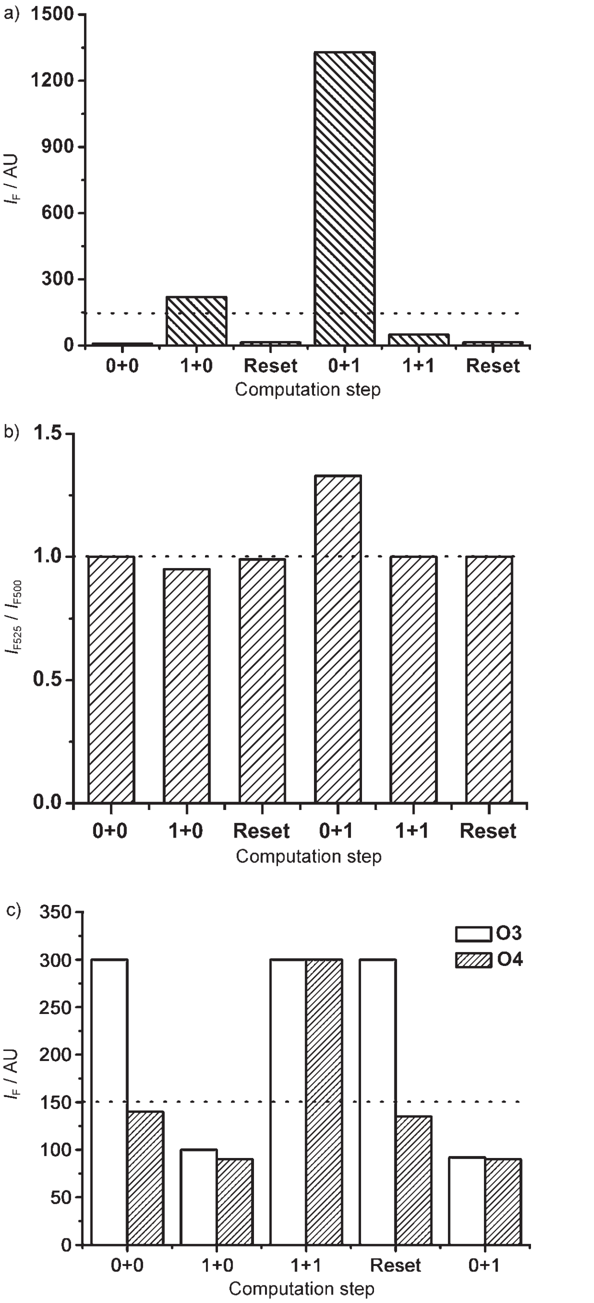


Figure 7. The computation and reset cycles of the half-subtractor for user 1 at a) the output channel at O1 and b) the output channel at O2. The reset process is achieved through the addition of TFA (0.1 M). The dotted line represents the threshold. c) The computation and reset cycles of the half-adder for user 2. The reset process is achieved through the addition of *n*-butylamine (0.8 M). The dotted line represents the threshold.

crofluidic devices, which will dramatically decrease the volume of consumption after a series of logic operations, such as authentication and algebraic execution. A chiplike device is easy for the fabrication of current chemically driven molecular platforms in potential use.[14b]

Conclusion

A secured molecular platform, capable of performing user-specific functionalities under protection, has been constructed with the aim of examining the security feature of molecular systems. User 1 is endowed with subtraction functionality, whereas user 2 is endowed with addition functionality (Figure 8). Each cannot access what the other can do. Although the present system is just a prototype device with limited functional complexity, it reveals a strategy on how to defend against information invasion at the molecular level. By activating some binding modes of the fluorescent switch, the fluorescent molecule can perform both authentication of user identities and execution of digital functionalities, which indicates that the functionality of a molecular device is immune to illegal access.

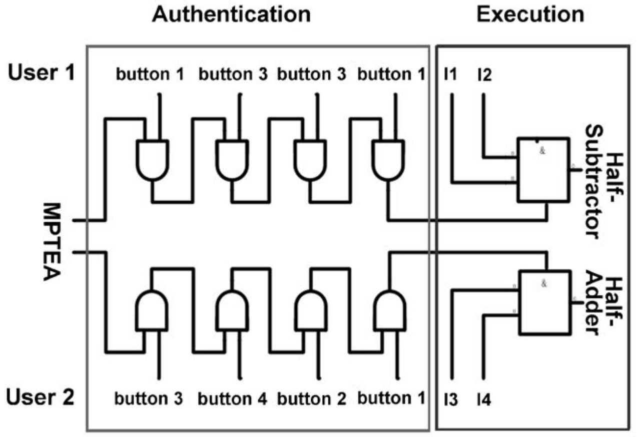


Figure 8. Illustration for the operational procedure of user-specific binary algebra.

The potential application of the present system may be found in the areas where the device functionalities are specific to the users' identities. The chemical basis of involved security policy, namely, the authentication-prior-to-execution strategy, is set up on the in situ conversion to activate the recognition reaction in a unique molecule, and can be extended to other chemical-based systems.[15] From password authentication to user-specific functionalities, molecular devices are improved with their security feature step by step. With decreased information risk, the prototype of a secured molecular platform may inspire a diverse potential application of small molecules and biomolecules in this fast developing information era.

Experimental Section

General methods: ^{1}H and ^{13}C NMR spectra were recorded on a Bruker ARX 400 MHz spectrometer. Chemical shifts are quoted in parts per million (ppm) and referenced to tetramethylsilane. IR spectra were recorded on a Nicolet 5MX-S infrared spectrometer. Elemental analyses (C, H, N) were performed on an Elementary Vario EL analyzer. Mass spectra were obtained on a VG ZAB-HS mass spectrometer and a Finnigan LCQ mass spectrometer. High-resolution mass spectra were measured on a Micromass ZAB-HS spectrometer.

Photophysical measurements: The fluorescence spectra were determined on a Hitachi F-4500 spectrophotometer at room temperature. All of the spectral characterizations were carried out in acetonitrile (HPLC grade) at room temperature within a 10 mm quartz cell. The execution of different logic functionalities, which includes authentication, binary algebraic calculation, encrypted communication, and information storage, was accomplished through the introduction of the appropriate chemical inputs into the quartz cell starting from a solution of MPTEA in acetonitrile.

MPTEA: [5-Methoxy-2-(2-pyridiyl)thiazoyl]ethyne (MPTE) was prepared following a previously reported procedure.[8] MPTE (109.6 mg, 0.51 mmol) and 4-iodoaniline (131.9 mg, 0.60 mmol) were dissolved in dry THF (20 mL) and purged with argon three times in the presence of [Pd(PPh_3)$_2$$Cl_2$] (17.7 mg, 0.25 mmol) and CuI (9.5 mg, 0.05 mmol). Triethylamine (5 mL) was injected into the reaction mixture and it was stirred overnight at room temperature under argon. The mixture was concentrated in vacuo and the residue was poured into water (20 mL) and extracted with dichloromethane three times. The organic phases were combined, washed with saturated aqueous NH_4Cl solution three times, dried over anhydrous Na_2SO_4, and evaporated to dryness. The crude product was purified by column chromatography with ethyl acetate/petroleum (1:1, v/v, R_f=0.6) as eluent. Yield: 90%; ^{1}H NMR ($CDCl_3$, 400 MHz): δ=8.54 (d, J=3.2 Hz, 1H), 8.14 (d, J=7.1 Hz, 1H), 7.76 (t, J=1.5 Hz, 1H), 7.40 (d, J=9.0 Hz, 2H), 7.27 (t, J=1.5 Hz, 1H), 6.63 (d, J=9.0 Hz, 2H), 4.15 (s, 3H), 3.84 ppm (s, 2H); ^{13}C NMR ($CDCl_3$, 100 MHz): δ=166.6, 153.9, 151.2, 149.1, 146.8, 136.9, 133.2, 124.0, 120.7, 118.9, 114.6, 112.2, 93.9, 79.0, 63.5 ppm; FTIR (KBr): $\tilde{\nu}$= 3472 (m), 3360 (s), 3211 (w), 3066 (w), 2921 (w), 2208 (m), 1625 (vs), 1604 (vs), 1537 (vs), 1511 (vs), 1437 (s), 1353 (vs), 1308 (s), 1243 (m), 1170 (m), 1025 (m), 953 (m), 775 cm^{-1} (m); HRMS: m/z calcd for $C_{17}H_{13}N_3OS$: 307.0779; found: 307.0783; elemental analysis calcd (%) for $C_{17}H_{13}N_3OS$: N 13.67, C 66.43, H 4.26; found: N 13.32, C 66.68, H 4.36.

Acknowledgements

The authors acknowledge the support for this research by the NSFC under contract numbers 20490213, 20221101, and 20423005, and by Peking University.

[1] a) A. P. de Silva, H. Q. N. Guaratne, C. P. McCoy, *Nature* **1993**, *364*, 42–44; b) L. M. Adleman, *Science* **1994**, *266*, 1021–1024; c) V. Balzani, M. Venturi, A. Credi, *Molecular Devices and Machines: A Journey into the Nanoworld*, Wiley-VCH, Weinheim, **2003**; d) A. P. de Silva, *Nat. Mater.* **2005**, *4*, 15–16; e) R. Beckman, E. Johnston-Halperin, Y. Luo, J. E. Green, J. R. Heath, *Science* **2005**, *310*, 465–468; f) J. E. Green, J. W. Choi, A. Boukai, Y. Bunimovich, E. Johnston-Halperin, E. DeIonno, Y. Luo, B. A. Sheriff, K. Xu, Y. S. Shin, H. -R. Tseng, J. F. Stoddart, J. R. Heath, *Nature* **2007**, *445*, 414–417.

[2] a) D. A. Parthenopoulos, P. M. Rentzepis, *Science* **1989**, *245*, 843–845; b) M. Irie, *Chem. Rev.* **2000**, *100*, 1685–1714; c) Y. C. Liang, A. S. Dvornikov, P. M. Rentzepis, *Proc. Natl. Acad. Sci. USA* **2003**, *100*, 8109–8112; d) J. Y. Jiang, S. Wang, W. F. Yuan, L. Jiang, Y. L. Song, H. Tian, D. B. Zhu, *Chem. Mater.* **2006**, *18*, 235–237; e) S. J. Lim, J. Seo, S. Y. Park, *J. Am. Chem. Soc.* **2006**, *128*, 14542–14547.

[3] a) D. Margulies, G. Melman, A. Shanzer, *Nat. Mater.* **2005**, *4*, 768–771; b) A. P. de Silva, M. R. James, B. O. F. McKinney, D. A. Pears, S. M. Weir, *Nat. Mater.* **2006**, *5*, 787–790; c) Y. C. Zhou, H. Wu, L. Qu, D. Q. Zhang, D. B. Zhu, *J. Phys. Chem. B* **2006**, *110*, 15676–15679; d) U. Pishel, *Angew. Chem.* **2007**, *119*, 4100–4115; *Angew. Chem. Int. Ed.* **2007**, *46*, 4026–4040, and references therein; e) J. Andréasson, S. D. Straight, S. Bandyopadhyay, R. H. Mitchell, T. A. Moore, A. L. Moore, D. Gust, *Angew Chem.* **2007**, *119*, 976–979; *Angew. Chem. Int. Ed.* **2007**, *46*, 958–961; f) A. P. de Silva, S. Uchiyama, *Nat. Nanotechnol.* **2007**, *2*, 399–410.

[4] a) M. N. Stojanovic, D. A. Stefanovic, *Nat. Biotechnol.* **2003**, *21*, 1069–1074; b) J. Macdonald, Y. Li, M. Sutovic, H. Lederman, K. Pendri, W. H. Lu, B. L. Andrews, D. A. Stefanovic, M. N. Stojanovic, *Nano Lett.* **2006**, *6*, 2598–2603; c) Z. Q. Guo, W. H. Zhu, L. J. Shen, H. Tian, *Angew. Chem.* **2007**, *119*, 5645–5649; *Angew. Chem. Int. Ed.* **2007**, *46*, 5549–5553.

[5] a) D. Margulies, C. E. Felder, G. Melman, A. Shanzer, *J. Am. Chem. Soc.* **2007**, *129*, 347–354; b) G. Strack, M. Ornatska, M. Pita, E. Katz, *J. Am. Chem. Soc.* **2008**, *130*, 4234–4235.

[6] a) P. B. Schneck, Proc. IEEE **1999**, *87*, 1239–1250; b) The White House, *Defending America's Cyberspace: National Plan for Information Systems Protection: Version 1.0: An Invitation to a Dialogue*, **2000**, http://www.libertysecurity.org/article729.html; c) B. Balacheff, L. Q. Chen, S. Perason, D. Plaquin, G. Proudler, *Trust Computing Platforms: TCPA Technology in Context*, Prentice Hall, Upper Saddle River, NJ, **2002**; d) S. Harper, P. Athanas, *Proceedings of the 37th Hawaii International Conference on System Sciences* **2004**, 1–8.

[7] A. Credi, *Angew. Chem.* **2007**, *119*, 5568–5572; *Angew. Chem. Int. Ed.* **2007**, *46*, 5472–5475.

[8] W. Sun, Y. R. Zheng, C. H. Xu, C. J. Fang, C. H. Yan, *J. Phys. Chem. C* **2007**, *111*, 11706–11711.

[9] J. L. Jensen, M. P. Gardner, *J. Phys. Chem.* **1973**, *77*, 1557–1562.

[10] M. H. Zheng, J. Y. Jin, W. Sun, C. H. Yan, *New J. Chem.* **2006**, *30*, 1192–1196.

[11] A. Coskun, E. Deniz, E. U. Akkaya, *Org. Lett.* **2005**, *7*, 5187–5189.

[12] R. Spillman, *Classical and Contemporary Cryptology*, Prentice Hall, Upper Saddle River, NJ, **2005**.

[13] a) C. T. Clelland, V. Risca, C. Bancroft, *Nature* **1999**, *399*, 533–534; b) A. Kishimura, T. Yamashita, K. Yamaguchi, T. Aida, *Nat. Mater.* **2005**, *4*, 546–549.

[14] a) A. W. Martinez, S. T. Philips, M. J. Butte, G. M. Whitesides, *Angew. Chem.* **2007**, *119*, 1340–1342; *Angew. Chem. Int. Ed.* **2007**, *46*, 1318–1320; b) S. Z. Kou, H. N. Lee, D. van Noort, K. M. K. Swamy, S. H. Kim, J. H. Soh, K. M. Lee, S. W. Nam, J. Y. Yoon, S. S. Park, *Angew. Chem.* **2008**, *120*, 886–890; *Angew. Chem. Int. Ed.* **2008**, *47*, 872–876.

[15] P. Ettmayer, G. L. Amidon, B. Clement, B. Test, *J. Med. Chem.* **2004**, *47*, 2393–2404.

Received: March 29, 2008
Published online: June 13, 2008