Chem Soc Rev

TUTORIAL REVIEW

View Article Online
View Journal | View Issue

Cite this: *Chem. Soc. Rev.*, 2018, 47, 2266

Molecules for security measures: from keypad locks to advanced communication protocols

J. Andréasson *[a] and U. Pischel *[b]

The idea of using molecules in the context of information security has sparked the interest of researchers from many scientific disciplines. This is clearly manifested in the diversity of the molecular platforms and the analytical techniques used for this purpose, some of which we highlight in this Tutorial Review. Moreover, those molecular systems can be used to emulate a broad spectrum of security measures. For a long time, molecular keypad locks enjoyed a clear preference and the review starts off with a description of how these devices developed. In the last few years, however, the field has evolved into something larger. Examples include more complex authentication protocols (multi-factor authentication and one-time passwords), the recognition of erroneous procedures in data transmission (parity devices), as well as steganographic and cryptographic protection.

Received 20th December 2017

DOI: 10.1039/c7cs00287d

rsc.li/chem-soc-rev

Key learning points
(1) Use of ion-sensitive, photochromic, and biomolecular systems as building blocks for molecular information technology.
(2) Chemical principles of molecular keypad locks.
(3) Advanced molecular logic functions for data communication.
(4) Design of molecular and supramolecular systems as security inks.
(5) Molecular data protection by encryption and steganography.

1 Introduction

The field of molecular logic deals with the use of stimuli-responsive chemical systems for the implementation of logic operations (AND, OR, INHIBIT, NAND, NOR, XOR, *etc.*) or the integrated operation of more complex logic circuits (half-adders, half-subtractors, encoders, decoders, *etc.*), in short to process information at the molecular level.[1–4] It is very tempting to relate these efforts to the ambitious objective of developing molecular computers in a bottom-up approach, thereby overcoming the limitations of the conventional production of silicon-based microprocessors. However, with time the community has realized that problems such as the concatenation of molecular logic devices or the improvement of their fan-out capacity constitute barriers that are not easy to overcome. As a consequence the field of molecular logic has developed into alternative directions, where such obstacles do not exist.[5] Nowadays, basic and advanced molecular logic operations are applied for the improved design of more selective drug delivery systems,[6] pro-drug activation,[7] theranostic molecular devices,[8] or the combinatorial sensing of analyte combinations.[9]

This Tutorial Review deals with a different use of molecules in the context of information technology. Rather than processing data through logic operations, molecular systems can be devised to protect, encode, encrypt, and conceal data. Ultimately all these activities lead to increased data security for their safer transport and communication. A typically chemistry-related example for these applications is security inks for protecting important documents or implementing anti-counterfeiting measures for example in banknotes.[10] Frequently, photochromic inks are used which offer two layers of protection: (a) the chemical identity of the compound itself and (b) the use of an external light trigger to make the ink visible. However, sophisticated chemical and structural analysis may reveal the nature of the ink. That is why important documents contain usually more than one security element to increase the difficulty of counterfeiting. A step ahead are security inks that react on combinations of external inputs, such as mechano-, electro-, thermo-, or photo-chromic compounds,[11,12] often offering luminescence as

[a] *Department of Chemistry and Chemical Engineering, Physical Chemistry, Chalmers University of Technology, SE-412 96, Göteborg, Sweden. E-mail: a-son@chalmers.se*
[b] *CIQSO-Centre for Research in Sustainable Chemistry and Department of Chemistry, University of Huelva, Campus de El Carmen s/n, E-21071, Huelva, Spain. E-mail: uwe.pischel@diq.uhu.es*

an additional reading (output) channel. Moreover, stimuli-responsive chemical systems that provide outputs in a non-linear and not straightforward predictable manner are ideal candidates for encrypting information.[13–15] In combination with sequential logic, which implements features such as password security, very powerful chemical approaches towards the safe communication of sensible information can be designed.[14] While this all may sound like good material for a fictional spy movie, the creative chemistry behind it is very serious and real, as will be illustrated in this Tutorial Review.

2 Early keypad locks

Everyone has practically daily contact with keypad lock devices. The simple act of retrieving money from an automatic teller machine or introducing a code for opening a door are examples for this statement. When performing these actions we need not only to know which buttons to press, but also in what order. In other words, the device has notion of the input history. This is achieved by so-called sequential logic operations. The principle of sequential logic and its tight connection with the creation of molecular memory functions have fascinated chemists for *ca.* 10 years.[16,17] In electronics a keypad lock is best understood as an *n*-input priority AND gate (PAND gate). Such a function is achieved by concatenation of *n* two-input AND gates that are connected by feedback coupling between the output of the previous AND gate $(n-1)$ and one of the inputs of the next AND gate (n).

How can one create sequence-dependent chemistry with a molecular system? A simple approach would be based on coupled chemical reactions. Let us say that compound A is to be transformed into a compound C in a two-step reaction with the intermediary product B. If we first add the reagent X that enables the A-to-B reaction and then logically transform the isolated B into C by means of a second reagent Y, we have a successful reaction sequence. If, however, we add first the second reagent Y, nothing or something else will happen as no B was present. The following reaction with reagent X may at best transform re-isolated A into B, but no C is obtained. This illustrates very well the chemical meaning of sequential operations. However, most approaches draw on metastable situations, based on kinetic differentiation, or bistable systems that can be addressed reversibly. In the following paragraphs this will be illustrated with early examples of molecular keypad locks that constitute proof-of-principle cases and form the fundament of more recent examples as discussed in Section 3. In order to benefit the reader by placing a specific emphasis on the tutorial aspects of this Review we have chosen to group the different keypad lock examples according to their conceptual and functional advance instead of classifying them by the underlying chemical mechanism.

The very first molecular keypad lock was devised by Margulies and Shanzer in 2007 (Fig. 1).[18,19] They were drawing on a pyrene/fluorescein FRET pair (FRET: Förster Resonance Energy Transfer) that is integrated in a dyad (**1**) by means of a siderophore-type linker, capable of Fe(III) complexation. On excitation of pyrene with UV light, FRET leads to green emission (525 nm) of the dianionic form of fluorescein in basic solution. However, this is only observed in the absence of Fe(III), which otherwise acts as an efficient fluorescence quencher. The metal cation can be removed by a competing chelate ligand, such as EDTA. This removal is kinetically differentiated depending on the pH of the solution. While at neutral pH EDTA acts readily with fast kinetics, the same process is slowed down at basic pH. This feature creates the required metastable situation for the implementation of a keypad lock function. Starting with the Fe(III)-complexed dyad at neutral pH (no emission at 525 nm), the addition of EDTA (decomplexation of Fe(III)) followed by the addition of base (generation of the fluorescein dianion) yields an emission output on addressing

J. Andréasson

Joakim Andréasson (1973) was awarded his PhD by the Chalmers University of Technology in 2002. He spent two years as a post-doctoral research fellow at Arizona State University and then returned to Chalmers starting his independent research group, supported by the award of an ERC Starting Grant (2007). Currently he is a Full Professor. His main research interests are related to the design of molecular photoswitches and their use in molecular logic and photo-pharmacology.

U. Pischel

Uwe Pischel (1973) obtained his PhD from the University of Basel in 2001. He spent time as a postdoctoral researcher at the Technical University of Valencia and then moved to the University of Porto to start his own research group. Since 2007 he has been working at the University of Huelva, where he is currently an Associate Professor in Organic Chemistry, holding as well the National Habilitation as a Full Professor (2015). He was awarded with the Grammaticakis-Neumann Prize of the Swiss Chemical Society in 2013. His main research interests are focused on molecular logic, supramolecular host–guest chemistry in water, and fluorescent probes for biomedical applications.

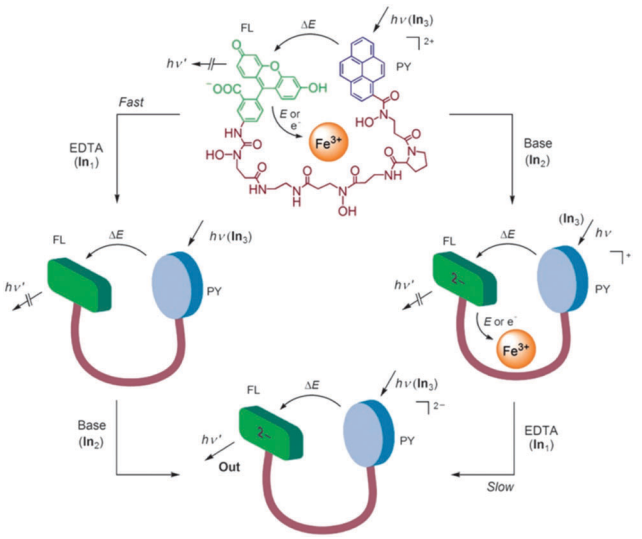

Fig. 1 Molecular keypad lock function based on the pyrene-siderophore-fluorescein conjugate **1** (structure on top). Reproduced from ref. 18 with the permission from Wiley.

the dyad with UV light. Adding first the base and then EDTA leads in principle to the same chemical situation, but due to the mentioned slower kinetics of Fe(III) decomplexation at basic pH, a considerable time lag of several hours is observed. Hence, measuring the output emission immediately after the successive addition of the inputs leads to a high emission only for one of the two input orders (first EDTA, then base). Considering UV light as the third input (that should be activated last), the password can be extended to even three digits.

The use of chemical inputs for the realization of chemical keypad locks was also favored by other groups. For example, Tian and co-workers coupled the known laser dye 4-dicyanomethylene-6-[4-(dimethylamino)styryl]-2-methyl-4*H*-pyran (DCM) with a pyridine-derived metal ion receptor (compound **2**; Fig. 2).[20] Complexation of Hg(II) cations yields fluorescence enhancement due to the blocking of photoinduced electron-transfer (PET) quenching by the receptor. However, Cu(II) cations have the opposite effect, being by themselves redox-active and causing electron transfer quenching of the DCM fluorescence. The sequential addition of the metal cations leads to different fluorescence outputs depending on the order of addition. Although the reasons are not experimentally corroborated, it is likely that kinetic control is responsible for this situation.

Other examples of chemically-addressable keypad locks include systems that use metal cations and anions as inputs[21,22] or imply the manipulation of a charge-transfer fluorophore (ICT; intramolecular charge transfer) by means of a chemical reaction as one input channel;[23] see for example compounds **3** and **4** (Fig. 2).

In principle, chemical keypad locks that build on the supramolecular recognition of ions could be operated in a reversible manner, allowing for resetting and recycling of the system. To achieve this, the introduced inputs would have to be neutralized or masked by the addition of counteracting chemicals.

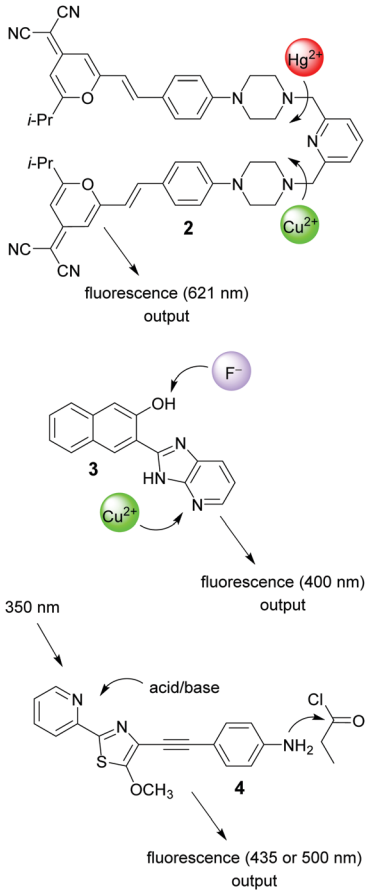

Fig. 2 Structures of molecular keypad locks **2–4** and their respective chemical inputs and emission outputs.

However, for the stable operation, even after many switching cycles, the accumulation of waste products that results from this practice constitutes a serious problem. This is why reversible light-induced processes were thought to be a worthwhile alternative.[24] Photoswitching introduces the required bistability for performing reversible sequence-dependent operations with photons of varying wavelengths as inputs. This has been realized either with systems that are operated solely with light, *i.e.*, in an all-photonic manner,[25,26] or with combinations of light and chemicals.[27–29] Herein, one example of each variation will be discussed in brief detail.

In 2015 the Pischel group devised a supramolecular keypad lock that is addressed by light and a chemical input (Fig. 3).[28] The formation of a homoternary complex of an anthracene derivative (**5**) with the macrocyclic host cucurbit[8]uril was employed to achieve a template effect in [4+4]photodimerization. This reaction was enabled by irradiation with light at $\lambda > 395$ nm. The photodimer can be decomplexed by addition of the strongly competing 1-aminoadamantane as a guest. Hence, irradiating first and then adding the competitor generates a free photodimer, which can be visualized by reversing the cycloaddition through irradiation at 254 nm and generating a fluorescent monomeric anthracene derivative. Contrarily, adding first the competitor and then shining light at $\lambda > 395$ nm leads to no photodimer,

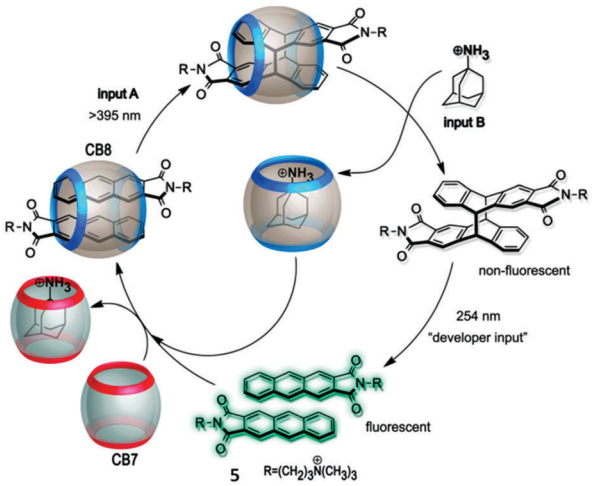

Fig. 3 Supramolecular keypad lock based on the photodimerization of guest **5** inside cucurbit[8]uril. Further, the recycling of the system by self-sorting is shown. Reproduced from ref. 28 with the permission from the Royal Society of Chemistry.

as the template effect of the cucurbituril is cancelled before irradiation. The system can be recycled by drawing on the chemical reversibility of supramolecular interactions and the self-sorting features of cucurbituril chemistry.

One step ahead is the exclusive use of light as inputs for molecular keypad locks. In 2011 the groups of Gust, Andréasson, and Pischel employed for this purpose the photochromic triad **6** (Fig. 4) that is composed of two distinct types of photoswitches: a fulgimide (FG) and a dithienylethene (DTE).[26] Both switches exist as an open (o) and a closed (c) isomer, which can be addressed either in a nearly orthogonal way, or simultaneously, depending on the wavelength that is chosen for operating the triad. In this way the solution can be highly enriched in all four isomeric forms: FGo–DTEo, FGc–DTEo, FGo–DTEc, and FGc–DTEc (note that the two FG units are treated as equivalent in this notation).

The closed fulgimide (FGc) is fluorescent, which can be conveniently used as the readout signal (output). However, in the FGc–DTEc conjugate the fluorescence is efficiently quenched by a FRET process with DTEc as an energy acceptor. In brief, using an input light of 366 nm (which isomerizes both the FG and the DTE photoswitches to their closed forms) and red light (which isomerizes selectively the DTEc form to the DTEo form), a keypad lock can be realized (Fig. 4). On the one hand, starting with the all-open form (FGo–DTEo) and irradiating first with 366 nm light and then with red light creates a fluorescent FGc–DTEo triad. On the other hand, inverting the order of light input application, *i.e.*, first red light (which has no effect on FGo–DTEo) and then 366 nm light, creates a non-fluorescent FGc–DTEc triad. The all-photonic character of this keypad lock is very attractive, as it enables waste-free, highly fatigue-resistant, and chemically reversible switching to achieve resetting and recycling of the operation. Noteworthily, this is not the first all-photonic keypad lock that was reported in the literature. A similar system **7** (Fig. 5) that was built on the DTE and FG photoswitches, but uses a porphyrin as a signaling

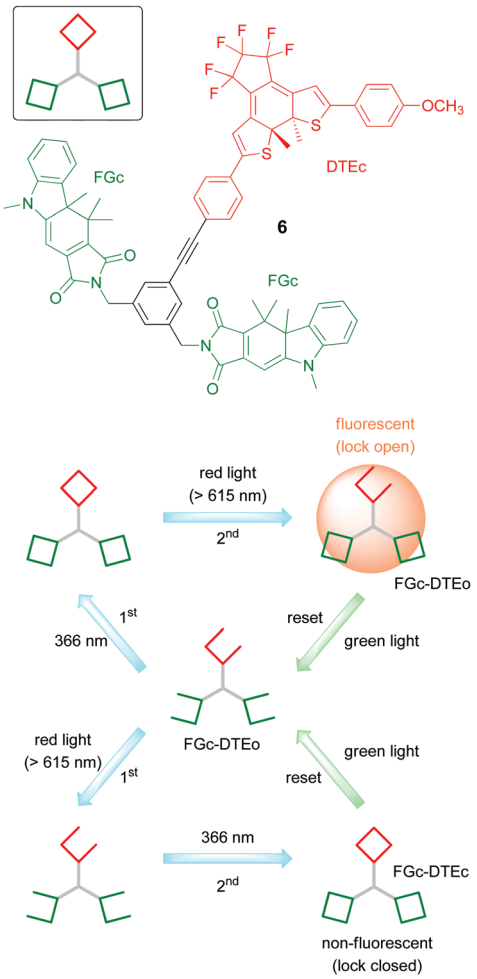

Fig. 4 Structure of the photochromic keypad lock **6** (top) and its working principle (bottom).

unit, was reported by the groups of Gust and Andréasson in 2009.[25]

With a view to the integration of logic operations with biochemical processes, the group of Katz has delivered several interesting examples of biomolecular keypad locks. In their first example (Fig. 6), dating back to 2008, they used concatenated AND gates to realize sequence-dependent enzymatic transformations.[30] The concatenation was achieved by defining the product output of a preceding transformation as the input of the next transformation. The sequentiality of enzyme addition was aided by immobilizing the enzymes on glass beads. Hence, they could be removed after completion of each enzymatic process, thereby avoiding false positives that would result from the accumulation of the different biocatalysts that were added in the wrong order.

In concrete, the enzyme invertase was used to transform sucrose into glucose (and fructose). The glucose was required by glucose oxidase to produce hydrogen peroxide and finally, the peroxide enabled the microperoxidase-11-catalyzed oxidation of the ABTS dye to yield a colorimetric output. Akin to the example that was given at the beginning of this Section, linking

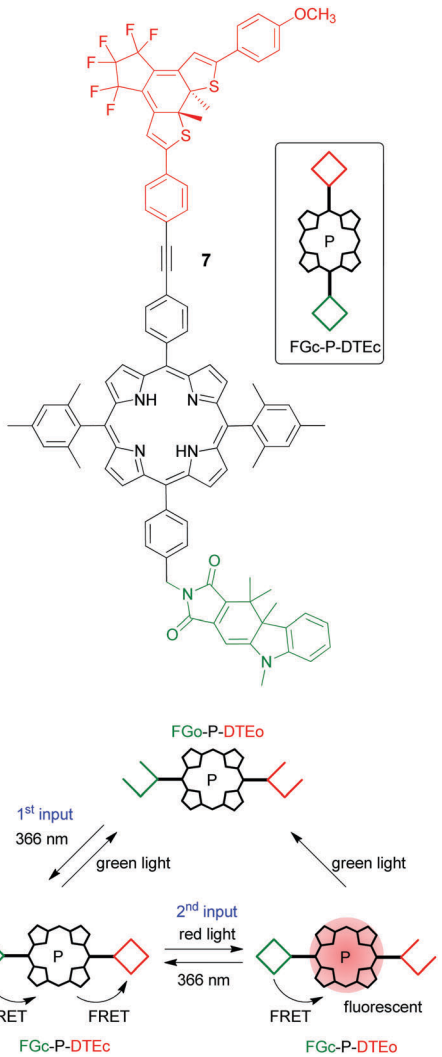

Fig. 5 Photochromic keypad lock **7** (top) and its working principle (bottom).

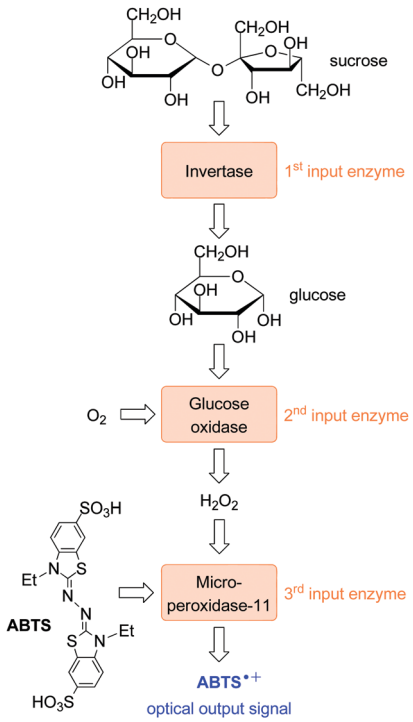

Fig. 6 Biomolecular keypad lock based on coupled enzymatic transformations.

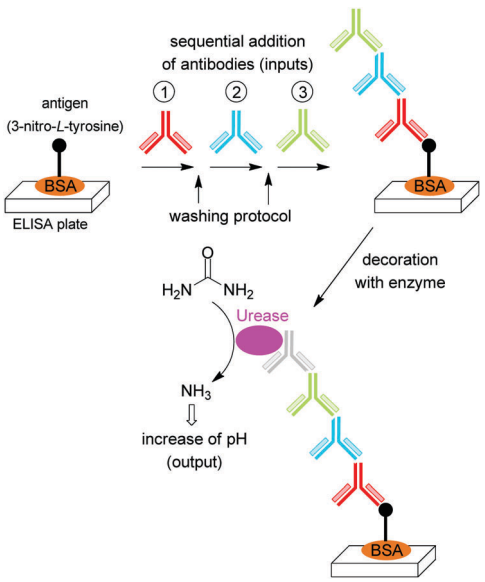

Fig. 7 Realization of a biomolecular keypad lock by sequential antibody assembly on a surface.

the action of the downstream enzyme-2 to the substrate–product conversion in an upstream enzyme-1-catalyzed step introduces the sequence dependency that is required for the operation of a keypad lock. A similar principle was used by the same group to activate a biofuel cell through a cascade of enzymatic reactions with the sequence characteristics as described above.[31]

In another work reported by the same group, sequentiality was introduced by the stepwise binding of complementary antibodies onto a surface (Fig. 7), the last one being labeled with an enzyme for a specific biocatalytic transformation for output generation.[32] Only if the correct antibody sequence is applied in consecutive labeling/washing steps the enzyme will be immobilized onto the surface. If the incorrect sequence is used in the protocol, the non-recognized antibody will be washed away. Again, this system was coupled to a biofuel cell, enabling the password authorization of the cell. A very similar principle based on the sequence-dependent hybridization of single-stranded oligonucleotides was used later (2013) by the Wang group; see Section 3.[33]

3 Advanced keypad locks and other authentication protocols

Before continuing the discussion about the keypad locks, now with a larger set of inputs, we would like to raise the question about the total number of input combinations for these devices. Starting out with the regular two-input AND gate,

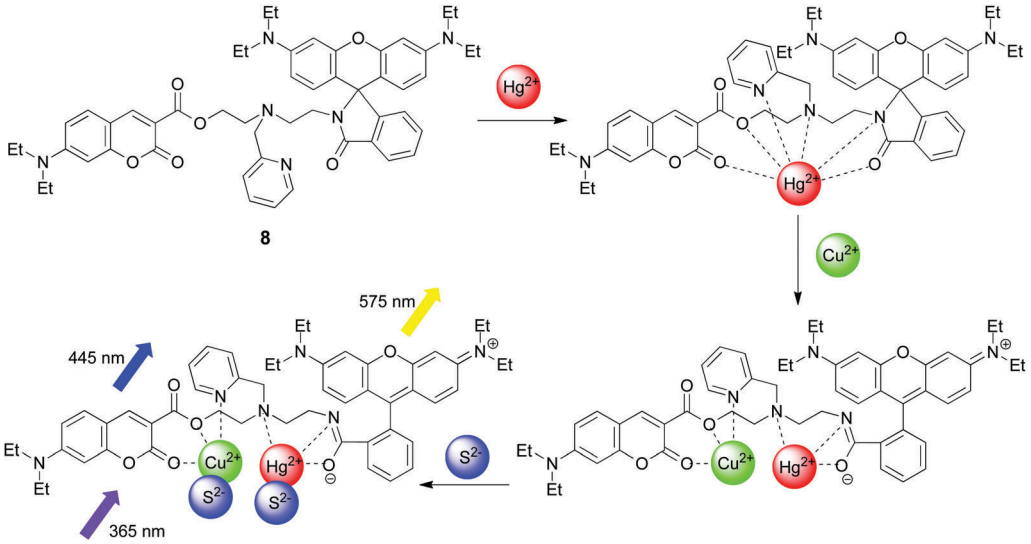

Fig. 8 Functional principle of the four-input keypad lock (**8**) based on coumarin and rhodamine fluorescence.

a combinational logic device where the input order does not matter, there are four possible input combinations: 00, 01, 10, and 11. In general terms, the *n*-input gate has 2^n input combinations. The two-input keypad locks are often compared to the two-input priority AND gate (PAND gate). As mentioned above, here not only the correct input combination matters, but also the order by which the inputs are applied. This implies in principle that the total number of ordered binary input combinations increases with the number of inputs *n* as $2^n \times n!$ (8 for a two-input device, 48 for a three-input device, 384 for a four-input device, *etc.*).† Thus, it is easily realized that an increased number of inputs follow an increase in the security.

In 2014, Ng and co-workers designed a molecular dyad (**8**), containing coumarin and rhodamine fluorophores, which performs as a four-input keypad lock (see Fig. 8).[34] The inputs used are Cu^{2+}, Hg^{2+}, and S^{2-} ions together with 365 nm UV excitation for the emission readout of the fluorescence outputs at 445 nm (coumarin fluorescence) and 575 nm (rhodamine fluorescence). Due to the large number of oxygen and nitrogen atoms incorporated into the fluorophores and the linker, several multi-dentate binding modes for the cations are offered. Intense emission from rhodamine at 575 nm is only observed for the ring-opened isomer, formed mainly upon the addition of Hg^{2+} followed by Cu^{2+}. This observation *per se* implies a two-input keypad lock. In order to realize the four-input version, S^{2-} ions were used as a third chemical input and 365 nm UV light for the emission readout was interpreted as being part of the inputs. Unless S^{2-} is added subsequent to the formation of a fluorescent ring-open isomer, it will coordinate to the cations and prevent the rhodamine ring-opening, required for intense emission (output on). UV exposure for emission readout must, of course, be applied as the final input. The coumarin fluorescence at 445 nm must also be read in order to distinguish between the input sequences $Hg^{2+} \rightarrow Cu^{2+} \rightarrow$ 365 nm UV and $Hg^{2+} \rightarrow Cu^{2+} \rightarrow S^{2-} \rightarrow$ 365 nm UV, being significantly higher for the latter input combination.

A clever means of realizing DNA-based keypad locks relies on the input-sequence dependent formation of toeholds.[33] Wang and co-workers used this approach to devise a five-input keypad lock schematically depicted in Fig. 9.[33] A single-stranded DNA oligonucleotide A is attached to a silver microsphere. Available as inputs are five single-stranded DNA oligonucleotides, herein referred to as A′B, B′C, C′D, D′E, and E′F. If A′B is added to A at the silver microsphere, the A′ segment will hybridize with A, as these sequences are complementary. Upon subsequent addition of B′C, the B′ segment hybridizes to the B toehold segment of A′B, leaving in turn the C segment as a toehold. Sequential addition of C′D, D′E, and E′F completes the assembly of the five input oligonucleotides. Hybridization between D′E and E′F leads to the formation of a G-quadruplex (G4) which together with hemin catalyzes the oxidation of TMB (tetramethylbenzidine) by H_2O_2 to yield the strongly blue colored species TMB^+, read as the output. As the silver microspheres are rinsed after each input application, the abovementioned input

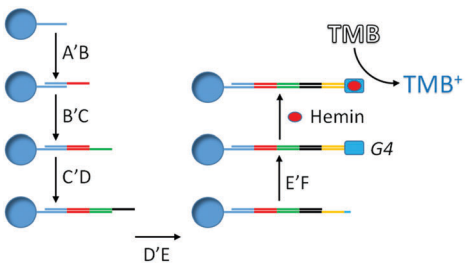

Fig. 9 Schematic representation of a five-input DNA-based keypad lock. Segments with the same colors indicate complementary sequences.

† It may be debatable whether or not setting input 1 = 0 followed by input 2 = 0 is different from the reversed input order. However, the arguments used in the text are definitely valid assuming that the user must make an active binary choice for each input.

sequence is the only one that results in the formation of the G-quadruplex and, hence, that switches the output to the on-state.

So far in this Tutorial Review, the molecular security devices were described as having a fixed single password, that is, there is only one input sequence that switches the output to the on-state. This implies that knowing the password is enough – the lock opens without caring about the identity of the user. In other words, authentication (verification of the user identity) cannot be done. Disregarding multi-factor authentication (see below) a system that allows also for user authentication must have at least as many different valid passwords as it has users. This is true also on the output side, that is, there must be at least as many unique output combinations that open the lock as there are users. This implies, of course, that a single output signal is not sufficient.

Wang and co-workers devised an electrochemical DNA-based system that can discriminate between two different authorized users.[35] Here, a single-stranded oligonucleotide L is anchored to a gold electrode (see Fig. 10). At the opposite end, L is decorated with a ferrocene (Fc) unit. Oligonucleotide A is partially complementary to L, hybridizing to L to form double-stranded LA. At this point, Fc is located too far away from the gold electrode, and no redox reactions are detected from the electrochemical current used as output 1. Upon addition of single-stranded oligonucleotide B (Input B), being completely complementary to A, double-stranded AB is formed and washed away from L. Upon subsequent addition of Hg^{2+} (Input M), L is folded into a hairpin structure, and Fc is brought in close proximity to the gold electrode resulting in the appearance of the redox signal at around 0.5 V in the electrochemical current. Output 1 is now switched to the on-state. Reversal of the input order implies that Hg^{2+} instead induces a hairpin at oligonucleotide A. After the addition of Input B, Hg^{2+} is washed away with double-stranded AB, implying that L can no longer form the hairpin required to bring Fc close to the electrode. No redox reaction occurs, and output 1 stays in the off-state.

The scheme described above is nothing but a regular two-input keypad lock. So, how could this be used to discriminate between two authorized users? The key lies in the usage of a second metal ion, Ag^{+}, as Input S. This ion is also capable of inducing the hairpin structure required for the function of the keypad lock. Moreover, Ag^{+} is electroactive itself, and gives rise to an additional oxidation peak at *ca.* 0.2 V that can be detected in the readout operation (output 2). This boils down to the following situation (illustrated with the two fictional characters Alice and Bob):[36] The password, or input sequence, of Alice is BM (oligonucleotide B followed by Hg^{2+}). Oxidation of Fc is observed at around 0.5 V, implying that the lock opens. The absence of the peak at 0.2 V tells the system that this is Alice. The password for Bob is instead BS (oligonucleotide B followed by Ag^{+}). Again, the Fc is oxidized at 0.5 V and the lock opens. In addition, the presence of the peak at 0.2 V identifies the user as Bob. In another example Yan and co-workers achieved the authentication of two users with their keypad lock **4** (Fig. 2) by reading different fluorescence emission output channels.[23] Dube and co-workers introduced a hemithioindigo photoswitch (**9**) that can be addressed by visible light and acid/base chemistry (see Fig. 11). The variation of the absorption output channel enabled the authentication of different users with the same system, albeit different initial states had to be used. Interestingly, in one of these signal configurations an automatic (thermally activated) closing of the lock was achieved.

Describing the outputs in binary terms (on or off) is by far the most adopted approach. An output signal above the threshold value grants access, whereas a signal below the threshold value denies access. Moreover, the optical outputs are mostly read at a single wavelength, implying that only a tiny fraction of the spectral information is being used. In 2013, Margulies and co-workers published a multi-fluorophore unimolecular keypad lock (**10**; Fig. 12), presenting a novel approach to the choice of outputs and inputs.[37] Rather than identifying a single wavelength

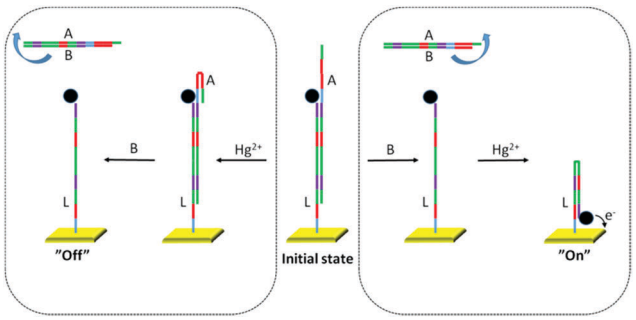

Fig. 10 Two-input DNA-based keypad lock with an electrochemical readout. Segments with the same colors indicate complementary sequences.

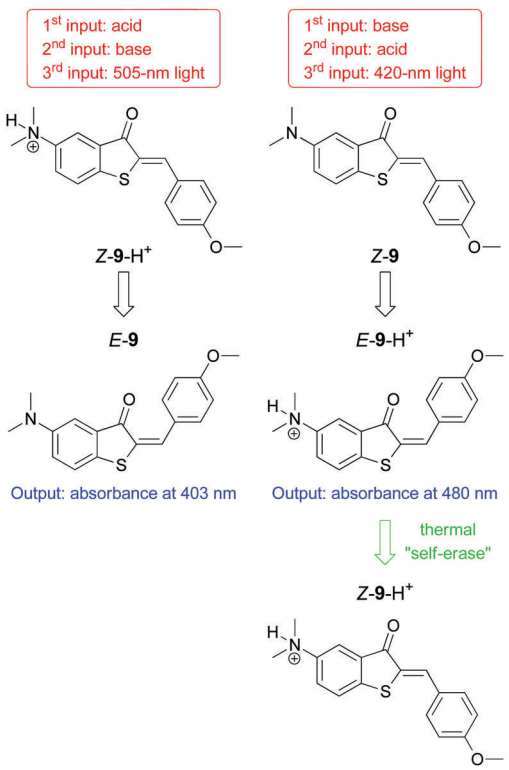

Fig. 11 Keypad lock function of the photoswitch **9**.

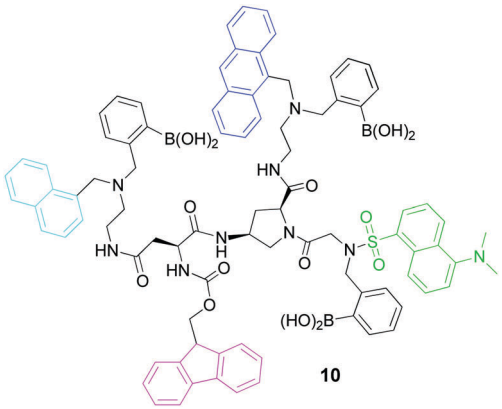

Fig. 12 Structure of the multi-fluorophore keypad lock **10**.

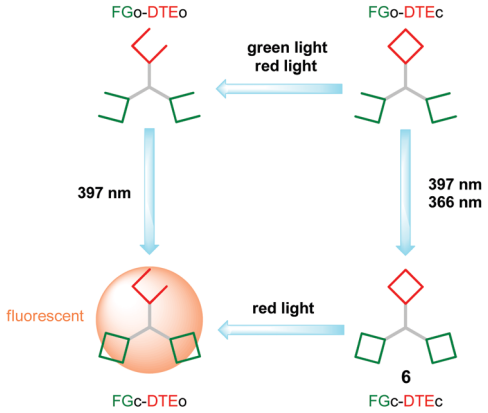

Fig. 13 Working principle of a keypad lock with a one-time password. See Fig. 4 for the structure of triad **6**.

where the optical signal is above the threshold for exclusively one input combination, they used principal component analysis (PCA) to process a 400 nm broad spectral region. Moreover, they abandoned the notion that exclusively one input combination will open the lock. Instead the focus was on identifying as many input combinations as possible that generate emission spectra different enough to make them "PCA-unique", that is, distinguishable after PCA analysis. With this approach, a large number of users can not only be authorized, but also authenticated by the system. In a later section of this Tutorial Review, a similar molecular system devised by the same group will be more comprehensively described in the context of secure data communication (Section 5).

No matter how secure a password is in terms of length *etc.*, it can never be safe from being recorded (stolen). This risk, however, is eliminated by the use of one-time-passwords (OTPs). As inferred by the name, OTPs are passwords that are changed after having been used once, so that any entry of a password stolen by intrusion will be unsuccessful. Conventional methods for OTP generation often implies the use of challenge-response pairs (see Section 5) where, *e.g.*, the bank is issuing a new challenge to the user for each transaction.

Andréasson and co-workers recently presented a study in which the user must apply first a regular "static" password followed by an OTP to be authorized.[38] The molecular platform used was the photochromic triad **6** displayed in Fig. 4 that was already discussed above as an all-photonic keypad lock. Key to the function is that only the FGc–DTEo isomer displays intense fluorescence, used as the output signal. From Fig. 13 it is seen that depending on the initial state, different light-exposure sequences must be applied for the formation of the fluorescent isomer. This implies that the "password" can be changed by simply resetting the triad to another initial state. The molecular system must somehow communicate to the user, in a secure manner, the new password. This opens up for the possibility to use also multi-factor authentication (see below). It is worth re-emphasizing that the all-photonic nature of the triad makes resetting and the application of the input combinations (passwords) totally waste free, as discussed above. On the downside, an obvious limitation is that triad **6** only offers a total of four isomeric forms, dramatically limiting the number of potential passwords.

We would like to round up this section with a discussion on multi-factor authentication. Two-factor authentication (2FA) qualifies as such, and is a procedure that enters into the everyday life of many people. The two factors here are typically something that the user has (*e.g.*, a bank card) and something that the user knows (*e.g.*, the PIN code, or a password). Biometrics is sometimes also used, reflecting something that is unique and inherent to the user (*e.g.*, finger prints, retina blood vessels pattern). A very basic step toward molecular emulation of 2FA was recently presented by Andréasson and co-workers,[38] but more sophisticated versions of multi-factor authentication are anticipated.[39] Here, biometrics will be the key player as the ultimate goal would be the continuous monitoring of analytes in the skin secretions of the user. It is foreseen that the concentration profile over time of 23 amino acids in the sweat would be sufficient for a pattern unique to each individual to be generated. In a later section (Section 5), we will give examples where 2FA is implicitly realized, given that a molecule or a molecular ensemble is considered as something that the user must have.[14]

4 Error detection in data transmission

The abovementioned approach to add more inputs (longer passwords) is certainly helping to improve the security of password-protected systems. However, increasing the lengths of the passwords (or any type of data string) increases the risk of erroneous procedures in the entry of the password/data. Erroneous procedures in the manual entry of data, or in the transmission thereof, could have serious consequences. Let us suppose that Bob wants to transfer money to his friend Alice. This operation typically includes the manual entry of Alice's bank account number, as well as the transmission of this data to the receiver (the bank). Both these processes could be inflicted by errors, that is, the money could potentially end up at a third person's bank account. This is why check digits are being introduced. These are extra digits added to the set of initial data in such a way that errors occurring in the entry or the transmission of the data will be detected. And errors do for

sure occur; the impressive rates at which data can be transferred today (TB per s) implies that if 1 out of 100 billion bits is corrupted, 10 errors would occur each second.

One example of a check digit is the parity bit (P). Parity bits are added to a string of binary data (D_n) so that the total number of 1s (Σ) is even (even parity). This operation is performed by the parity generator. The herein generated data string D_nP is now transmitted to the receiving end, where the parity of the data string has to be checked. This is performed by the parity checker. If the parity is still even, fault-free data transmission has (likely) occurred,‡ whereas if the parity is odd, the checker communicates this to the user. This communication occurs through the output from the parity checker. A "0" output signals that data transmission is OK, whereas a "1" output implies that errors have occurred. To exemplify, if two bits of data (D_1 and D_2) are to be transmitted, where $D_1 = D_2 = 1$, the generated parity bit P will be a 0 to yield the string D_1D_2P = 110. If the string reads 100 after transmission, the output from the checker will be 1. For a 2-bit parity generator, where the original set of data consists of two bits, D_1 and D_2, the parity generator performs the function of an exclusive OR (XOR) gate according to Table 1. The corresponding truth table of the parity checker is shown in Table 2.

The first example of a molecule-based parity generator/checker was reported by the groups of Pischel and Andréasson in 2013.[40] Two photochromic triads were used in this study, each performing the correct parity functions: the above described triad **6** (Fig. 4) and triad **11** (Fig. 14). Both constructs consist of fulgimide (FG) and dithienylethene (DTE) photoswitches. Triad **6** carries two identical FG units and a single DTE unit, whereas triad **11** has one FG unit and two DTE units. As indicated above, the only situation where intense emission is observed from these triads is when FG is in the closed isomeric form FGc, and DTE is in the open isomeric form DTEo. Initially, the triads are set to the FGo–DTEo form, displaying no detectable emission under exposure to 380 nm light. The effect of extended irradiation with 380 nm light on the isomeric distribution is the closing of both photoswitches to generate the non-fluorescent FGc–DTEc form, highly enriched in the photostationary state (PSS). However, seminal for the function is that *en route* to the FGc–DTEc-enriched PSS, the triads pass over a situation where the samples are enriched in the FGc–DTEo fluorescent isomer (see Fig. 14). Thus, in terms of an XOR-gate with a fluorescence readout, this is the state to be generated after application of exclusively one of the two inputs.

Defining both degenerate input signals D_1 and D_2 as 380 nm UV light, and the output as FGc fluorescence at 630 nm results in the corresponding XOR logic: with no inputs applied, the triads are in the non-fluorescent FGo–DTEo form. D_1 or D_2 alone is sufficient to enrich the samples in FGc–DTEo and the output is switched on, whereas the application of both D_1 and D_2 brings the sample very close to the PSS, containing mainly the non-fluorescent FGc–DTEc isomer. At any time during the cycle, the triads can be conveniently reset to the initial FGo–DTEo form by exposure to visible light. For the triads to perform the function of the somewhat more complex parity checker, light at $\lambda > 540$ nm has to be defined as the additional

‡ It is inherent to the function of the described parity devices that if two (or an even number) errors occur, the checker won't be able to detect the erroneous procedures.

Table 1 Truth table for a 2-bit parity generator

	Inputs		Output	
Entry	D_1	D_2	P	Σ^a
1	0	0	0	0, even
2	0	1	1	2, even
3	1	0	1	2, even
4	1	1	0	2, even

[a] Number of 1s in the D_1D_2P string.

Table 2 Truth table and result of a 3-bit parity checker

	Inputs			Output		
Entry	D_1	D_2	P	C	Σ^a	Result
1	0	0	0	0	0, even	Ok
2	0	1	0	1	1, odd	Error
3	1	0	0	1	1, odd	Error
4	1	1	0	0	2, even	Ok
5	0	0	1	1	1, odd	Error
6	0	1	1	0	2, even	Ok
7	1	0	1	0	2, even	Ok
8	1	1	1	1	3, odd	Error

[a] Number of 1's in the D_1D_2P string.

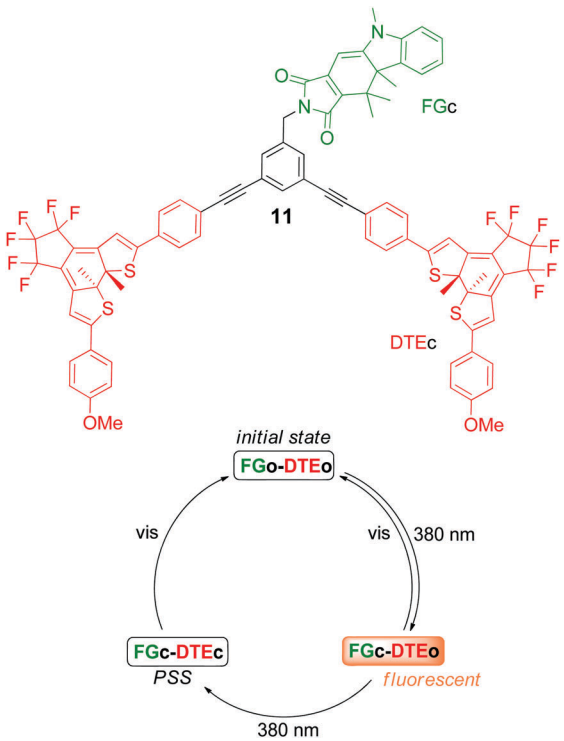

Fig. 14 Structure of the all-photonically switchable triad **11** (top) and the working principle that leads to the function of a parity checker (bottom). The same functionality can be achieved with triad **6**.

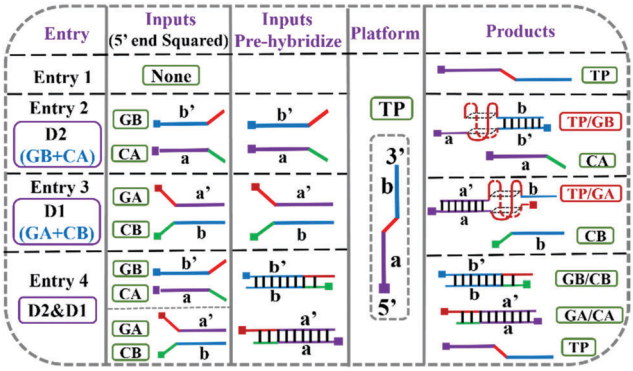

Fig. 15 Representation of the hybridization scheme of a DNA-based parity device. Shown is also the resulting formation (entries 2 and 3) or no formation (entries 1 and 4) of the G4 quadruplex. Reproduced from ref. 41 with the permission from the Royal Society of Chemistry.

input, whereas the output again is read as the emission intensity at 630 nm.[40]

A cleverly designed DNA-based system performing the same functions was reported by Dong and co-workers.[41] Here, the parity generating/checking relies on the formation of G-quadruplexes (G4) following the addition of single-stranded input DNA oligomers to a single-stranded oligomer platform TP (see Fig. 15). The formation of G4 can be monitored spectroscopically and used as the output due to that the fluorescence intensity of a porphyrin reporter is dramatically increased upon binding to G4. Alternatively, the G4-dependent oxidation of TMB to deeply colored TMB^+ allows for naked eye detection. Input D_1 is defined as the addition of single-stranded GA and CB, whereas input D_2 is the addition of single-stranded GB and CA (see Fig. 15). Input D_1 alone switches the output on, as hybridization of the a′ sequence on GA to sequence a on TP yields G4. This is also true for Input D_2 alone, due to the hybridization between b′ on GB and b on TP. In contrast, applying both D_1 and D_2 does not switch the output on as hybridization instead occurs between the input strands, leaving the platform TP unhybridized, and G4 is not formed. This results in the XOR-gate logic required for parity generation. The corresponding parity checker was devised by introducing additional input strands to the system.

Parity checking can only detect errors, as one cannot infer from the output which position the corrupted bit has in the transmitted data string. Error correction requires the inclusion of more than one parity bit, and also that the parity of several different combinations of the bits in the transmitted string is being checked by, *e.g.*, the use of Hamming-codes. To the best of our knowledge, this matter has not yet been tackled on the molecular scale.§

§ Molecular parity devices with self-correcting capacities have been suggested (ref. 41). The approach used in these studies has been to change any checker output = 1 to output = 0 as default. However, this procedure cannot detect/correct the erroneous bit in the transmitted data string, it is only "silencing" the alert given by the parity checker.

5 Secure data communication

Encryption and authentication protocols

By the use of encryption, information is encoded to a protected form so that it cannot be read until after the corresponding decryption process. The information before encryption is referred to as the plaintext, and the cipher is the method (algorithm *etc.*) used in the encryption process, converting the plaintext into the ciphertext. A very trivial, yet illustrative example of a cipher is the Caesar shift, named after (and allegedly also used by) Julius Caesar. It implies that every letter in the plaintext is replaced by the letter shifted down the alphabet by a fixed number. For example, using a shift of three would encrypt the plaintext "ENIGMA" to the ciphertext "HQLJPD". The reverse operation converts the ciphertext back to the plaintext again in the decryption process. So, in order for Alice and Bob to communicate in a "secure" manner, they have to agree on the number of letters their text should be shifted, and then keep this number as their "secret".

This trivial cipher implies very weak security, as it can be easily broken using frequency analysis. In modern cryptography the security is dramatically strengthened by the use of highly complex encryption algorithms in combination with so-called keys. Today's encryption algorithms are by no means the "secret", but you must assume that any eavesdropper knows which one you are using. The secret is instead Alice's and Bob's key,[36] *e.g.*, a 56-bit number, that is merged together with the plaintext and crunched by the encryption/decryption algorithm. Unless you know this 56-bit number, the ciphertext cannot be decrypted (without brute-force attacks).

This scheme is also applied in authentication protocols. Suppose that that Alice wants to share information with Bob. Before doing so, she wants to make sure that it is really Bob that is on the other side of the communication line. Simply asking "Hey, who are you?" or "What is our password?" is not safe, due to the risk of eavesdropping. Instead, Alice asks Bob to encrypt a plaintext into the corresponding ciphertext using their mutual key. This is referred to as the challenge. Bob sends the ciphertext to Alice as the response, and Alice compares the ciphertext generated by Bob to the ciphertext that Alice also generates. If they match, Bob is authenticated. Please note the similarity between a challenge-response pair (CRP) and the input–output of a conventional logic gate. The main difference using this analogy, however, is that it should be practically impossible to infer the truth table of the logic gate in the case of CRP. Or in other words, even with a very large number of CRPs at hand, it should be practically impossible to find the key. Thus, this procedure compares practically to a one-way function.

Molecule-based encryption

Suppose that Alice and Bob decide to devise a perylene-based cryptographic key. The challenge could then be "1.2" (prepare a 1.2 μM perylene solution in cyclohexane and measure the absorbance at the band maxima at 387 nm, 408 nm, and 435 nm). The response would be the absorbance values. This trivial key offers very limited security, as there is a linear

relationship between the concentration and the absorbance values (challenge and response). Moreover, there is also a fixed relation between the absorbance at the three wavelengths. Any eavesdropper collecting a couple of CRPs would find the relation between the challenge and the response (in principle the molar absorption coefficients of perylene in cyclohexane at these three wavelengths). Finally, cloning of the key would not present a major challenge, as any attacker with sufficient knowledge in chemistry may simply identify a stolen key as perylene from NMR spectroscopy, mass spectrometry, or a qualified guess based on the UV-vis spectral features.

From the example above it is easily realized that any molecule-based cryptographic key must offer a highly non-linear relation between the challenge and the response. A very elegant example along these lines is the resonance energy-transfer (RET, equivalent to FRET) approach presented by Dwyer and co-workers, schematically depicted in Fig. 16.[42] In the demonstrated examples, grid-like DNA scaffolds containing more than 6000 bases are labeled with a set of different Alexa dyes to constitute the so-called RET keys. The Alexa dyes, and their individual positions, are chosen so that FRET processes can occur between them on the individual RET-keys. As the FRET efficiency is very sensitive to the distance and the orientation between the FRET donor and the FRET acceptor, small variations in the positions of the dyes will influence how they exchange excitation energy, which in turn will be reflected in the overall multi-exponential fluorescence decays of the dyes (lifetimes and amplitudes).

The overall fluorescence decay traces depend not only on the relative positions between the dyes, but also on the excitation and the emission wavelengths. In addition, the authors used different excitation delays (the time at which the excitation pulses hit the sample). Altogether, this allows for more than 23 000 unique CRPs per RET-key. As the cascade-like multi-FRET reactions occurring on each RET-key make it extremely hard to describe the overall fluorescence decay (output or response) as a function of the excitation event (input or challenge), the process is indeed comparable to a mathematical one-way function. In combination with the huge number of distinct RET keys (estimated to 10^{125}), any attempt of an attacker to simulate the FRET processes using all possible CRPs and RET keys in a brute-force attempt would be highly unfeasible. The authors estimate that the time required to do so would amount to 10^{340} (!) years.

The Margulies group published in 2016 an intriguing paper on the use of their multi-fluorophore/multi-receptor concept for encrypting, concealing, and protecting messages with the aid of molecular action.[14] Akin to the approach that was used by the same group for setting up combinatorial multi-analyte chemosensors[43] and keypad locks (see Section 3),[37] they introduced deliberately a very low degree of analyte selectivity in their molecular platform (**12**), termed as molecular-scale messaging sensor (m-SMS); Fig. 17. Several fluorophores, such as fluorescein, sulforhodamine B, and Nile Blue, were combined with receptors for cations (dipicolylamine), anions (thiourea and sulfonamide), and neutral molecules (boronic acid for sugar binding). In conjunction with FRET, photoinduced electron transfer and charge transfer as excited state communication mechanisms and their distance-dependent modulation as a function of the interaction of the m-SMS with chemical inputs, a highly non-linear fluorescence response is obtained. The complexity and number of different encryption keys are further increased by the fact that the type and concentration of the inputs, the concentration of the m-SMS, and the output detection conditions can be varied over a wide range. The obtained spectral fingerprints can be translated into numeric codes, constituting the encryption key that is used to cipher the plaintext, previously converted by a public key into a numeric code. The encryption feature can be combined with the above described password protection (Section 3), yielding only a meaningful message for the application of the correct input order. Finally, the m-SMS can be absorbed on ordinary letter paper, thereby hidden, and later on recovered by extraction. This third protection layer of the message is known as steganography.

Another way of introducing a non-linear response in chemical systems is the use of coupled supramolecular equilibria. This was developed by the Stoddart group in 2015.[13] They presented a

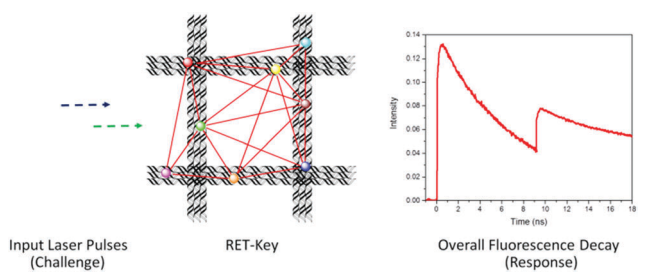

Fig. 16 Schematic depiction of the RET-key function. Red lines in the RET-key indicate the cascade-like FRET processes between the appended fluorophores, allowing for a highly non-linear relation between the challenge and the response. Adapted from ref. 42.

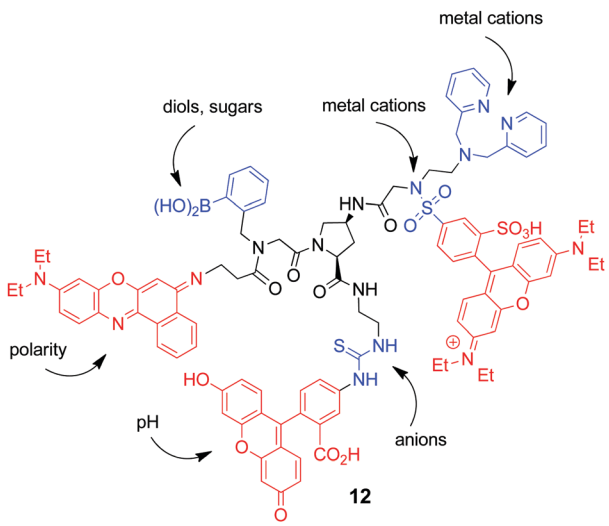

Fig. 17 Structure of the molecular-scale messaging sensor platform **12**. Identified are the fluorophore units (red) and the principal stimuli together with potential recognition sites (blue).

tunable solid-state supramolecular system that was based on a hetero[4]rotaxane (**13**, Fig. 18), formed by an axle consisting of a central diazaperopyrenium dication and pyrene-derived terminal units. The central part of the axle is complexed by γ-cyclodextrin that is flanked by two cucurbit[6]uril macrocycles. The latter are used to create a template effect in a click reaction required for the construction of the axle. The fluorescence emission of the solid-state materials is controlled by efficient FRET from the pyrene stoppers to the central pyrenium dication and the formation of excimers (between pyrenium ions) and/or exciplexes (between pyrenium and pyrene units) upon aggregation (Fig. 18). It was found that also the type of paper, on which the supramolecular material is supported, plays a role. The aggregates can be disassembled by the addition of extra γ-cyclodextrin that interacts with the pyrene stoppers (Fig. 18). This can be reversed by addition of competitor guests for the sugar macrocycle, such as adamantane derivatives. Hence, the emission spectra can be continuously tuned between the structured pyrenium monomer fluorescence (λ_{max} = 510 nm; Φ_f = 0.43) and the broad fluorescence of the different dimeric excited state complexes (λ_{max} = 610 nm, Φ_f = 0.08). The intricate coupling and competition between the different supramolecular equilibria (host–guest complexation between the pyrene unit and γ-cyclodextrin and aggregation) leads to a variable emission response. This response is a non-linear function of the concentrations of the different ingredients (heterorotaxane, cyclodextrin, and competitor), the binding constant of the competitor, and the paper support. The degree of complexity and emission color diversity can be additionally incremented by using fluorescent competitor guests (adding blue to the color palette) or quenchers. The fruitful combination of coupled supramolecular multi-equilibria and the intimately linked variation of photophysical phenomena was employed for the encryption and protection of data as well as the authentication of messages and users.

Another supramolecular ink published by Guo and collaborators builds on similar principles as discussed for the example by the Stoddart group.[15] They used a combination of three dyes (thioflavin T, Nile Red, and a pyrene derivative) and two co-assembled hosts (a cyclodextrin and a calixarene). Besides the occurrence of multiple host–guest equilibria, the implication of two-step FRET processes contributes to the desired non-linear emission response. In addition, the variation of the excitation wavelength was used as a diversification factor.

Materials other than supramolecular systems have also been employed to achieve encryption and decryption with advanced security levels. Among them are phosphorescent iridium(III) complexes that in conjunction with a boron dipyrromethene dye (Bodipy dye) can be used to encrypt data *via* a combination of fluorescence lifetime imaging and time-gated phosphorescence detection.[44] Furthermore, pyrene-tagged thymine- and cytosine-like structures, able to form dimeric complexes with Hg(II) and Ag(I), were used to encrypt chemical information.[45] Noteworthily, the Keinan group presented an interesting approach for exploiting parallel computing with DNA as a means for the encryption of images.[46]

Finally it should be mentioned that encoding, which is closely related to encryption, has been achieved with a series of interesting molecular approaches. While encoding transforms data into another format, encryption does the same but with the peculiarity that the reverse process can be only accomplished by specifically authenticated individuals. Some examples that illustrate encoding with molecular systems are mentioned in the following. Encoding of optical signals was successfully achieved by the Tian group by employing the

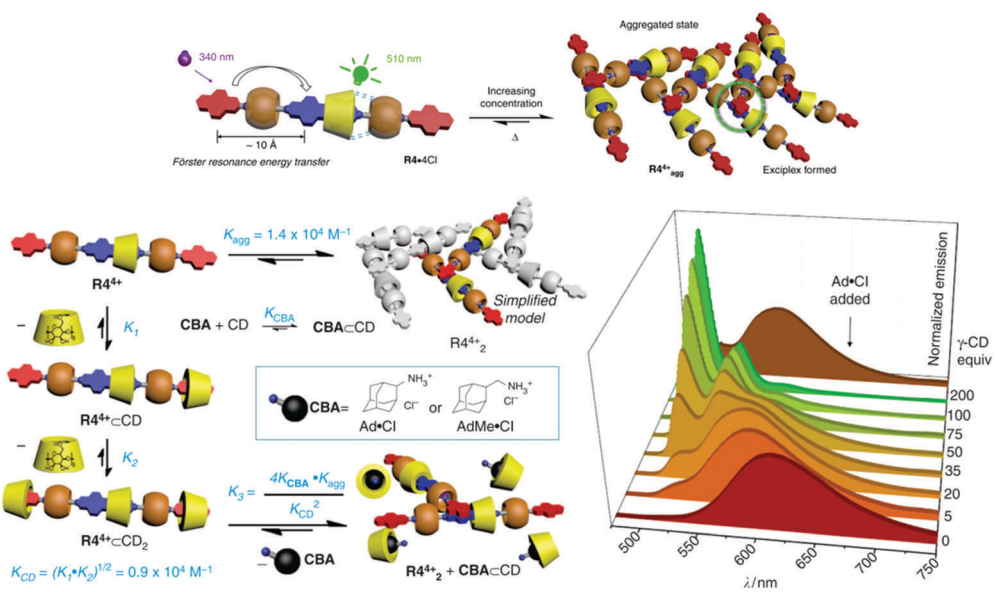

Fig. 18 Schematic depiction of the hetero[4]rotaxane **13** (**R4**$^{4+}$ in the figure), its main photophysical and supramolecular properties, and the stimuli responsive tuning of the emission color. The image is a composite of the original Fig. 1c, 3a and b from ref. 13. The original images by Hou *et al.* are licensed under CC BY 4.0.

photoswitching of bis(dithiazole)ethenes.[47] Keinan and coworkers encoded the chemical information contained in mixtures of aromatic compounds by high-precision recording of their proton NMR spectra.[48] In relation with bioelectrocatalytic processes it was shown by the Katz group that the electrocatalytic reduction of oxygen can be used to generate barcodes.[49] A set of relatively simple logic operations can also be used to encode large populations of micro-objects as shown by the de Silva group.[50]

6 Conclusions

From the examples discussed above, it is obvious that research in molecular information security is very inclusive. This is due to the fact that the chemistry underlying the realization of all these devices is highly multi-faceted, spanning organic chemistry, analytical chemistry, biochemistry, materials chemistry, supramolecular chemistry, photochemistry/photophysics, spectroscopy, DNA technology, and more. It is also clear that despite the combined efforts of all these researchers, the herein presented material must still be considered as proof-of-principle examples. That said, designing molecular systems for the protection of information is not presenting as many hurdles as the corresponding task for processing of information does. This follows from the fact that in order to process information on the molecular scale, the constructs should be designed so that any change in the state of the inputs must have a predictable and well-defined effect on the corresponding outputs. Several directed concatenation steps would typically be required for mimicry of the highly complex logical operations performed by today's silicon-based counterparts.[4] This should be contrasted to the desired non-linear (non-predictable) response between the ''inputs'' and the ''outputs'' of the security devices used for, *e.g.*, encryption and authentication. It is easily realized that the design of such systems is less challenging, as chaos appeals to molecules.

Conflicts of interest

There are no conflicts to declare.

Acknowledgements

We thank the Swedish Research Council VR (grant 2016-03601 for J. A.), the Spanish Ministerio de Economía, Industria y Competitividad (grant CTQ2014-54729-C2-1-P for U. P.), the ERDF, and the Junta de Andalucía (P12-FQM-2140 for U. P.) for generous financial support.

Notes and references

1 A. P. de Silva and S. Uchiyama, *Nat. Nanotechnol.*, 2007, **2**, 399–410.
2 K. Szaciłowski, *Chem. Rev.*, 2008, **108**, 3481–3548.
3 J. Andréasson and U. Pischel, *Chem. Soc. Rev.*, 2010, **39**, 174–188.
4 J. Andréasson and U. Pischel, *Chem. Soc. Rev.*, 2015, **44**, 1053–1069.
5 E. U. Akkaya, E. Katz and U. Pischel, *ChemPhysChem*, 2017, **18**, 1665–1666, Special Issue on Molecular Logic.
6 S. Angelos, Y. W. Yang, N. M. Khashab, J. F. Stoddart and J. I. Zink, *J. Am. Chem. Soc.*, 2009, **131**, 11344–11346.
7 S. Erbas-Cakmak and E. U. Akkaya, *Angew. Chem., Int. Ed.*, 2013, **52**, 11364–11368.
8 S. Erbas-Cakmak, O. A. Bozdemir, Y. Cakmak and E. U. Akkaya, *Chem. Sci.*, 2013, **4**, 858–862.
9 D. C. Magri, G. J. Brown, G. D. McClean and A. P. de Silva, *J. Am. Chem. Soc.*, 2006, **128**, 4950–4951.
10 E. L. Prime and D. H. Solomon, *Angew. Chem., Int. Ed.*, 2010, **49**, 3726–3736.
11 S.-J. Yoon, J. W. Chung, J. Gierschner, K. S. Kim, M.-G. Choi, D. Kim and S. Y. Park, *J. Am. Chem. Soc.*, 2010, **132**, 13675–13683.
12 K. Li, Y. Xiang, X. Y. Wang, J. Li, R. R. Hu, A. J. Tong and B. Z. Tang, *J. Am. Chem. Soc.*, 2014, **136**, 1643–1649.
13 X. S. Hou, C. F. Ke, C. J. Bruns, P. R. McGonigal, R. B. Pettman and J. F. Stoddart, *Nat. Commun.*, 2015, **6**, 6884–6892.
14 T. Sarkar, K. Selvakumar, L. Motiei and D. Margulies, *Nat. Commun.*, 2016, **7**, 11374–11382.
15 Z. Xu, D. Gonzalez-Abradelo, J. Li, C. A. Strassert, B. J. Ravoo and D.-S. Guo, *Mater. Chem. Front.*, 2017, **1**, 1847–1852.
16 U. Pischel, *Angew. Chem., Int. Ed.*, 2010, **49**, 1356–1358.
17 G. de Ruiter and M. E. van der Boom, *J. Mater. Chem.*, 2011, **21**, 17575–17581.
18 A. Credi, *Angew. Chem., Int. Ed.*, 2007, **46**, 5472–5475.
19 D. Margulies, C. E. Felder, G. Melman and A. Shanzer, *J. Am. Chem. Soc.*, 2007, **129**, 347–354.
20 Z. Q. Guo, W. H. Zhu, L. J. Shen and H. Tian, *Angew. Chem., Int. Ed.*, 2007, **46**, 5549–5553.
21 S. Kumar, V. Luxami, R. Saini and D. Kaur, *Chem. Commun.*, 2009, 3044–3046.
22 Q. Zou, X. Li, J. J. Zhang, J. Zhou, B. B. Sun and H. Tian, *Chem. Commun.*, 2012, **48**, 2095–2097.
23 W. Sun, C. Zhou, C.-H. Xu, C.-J. Fang, C. Zhang, Z.-X. Li and C.-H. Yan, *Chem. – Eur. J.*, 2008, **14**, 6342–6351.
24 D. Gust, J. Andréasson, U. Pischel, T. A. Moore and A. L. Moore, *Chem. Commun.*, 2012, **48**, 1947–1957.
25 J. Andréasson, S. D. Straight, T. A. Moore, A. L. Moore and D. Gust, *Chem. – Eur. J.*, 2009, **15**, 3936–3939.
26 J. Andréasson, U. Pischel, S. D. Straight, T. A. Moore, A. L. Moore and D. Gust, *J. Am. Chem. Soc.*, 2011, **133**, 11641–11648.
27 P. Remón, M. Hammarson, S. M. Li, A. Kahnt, U. Pischel and J. Andréasson, *Chem. – Eur. J.*, 2011, **17**, 6492–6500.
28 C. Parente Carvalho, Z. Domínguez, J. P. Da Silva and U. Pischel, *Chem. Commun.*, 2015, **51**, 2698–2701.
29 F. Kink, M. P. Collado, S. Wiedbrauk, P. Mayer and H. Dube, *Chem. – Eur. J.*, 2017, **23**, 6237–6243.
30 G. Strack, M. Ornatska, M. Pita and E. Katz, *J. Am. Chem. Soc.*, 2008, **130**, 4234–4235.
31 J. Halámek, T. K. Tam, G. Strack, V. Bocharova, M. Pita and E. Katz, *Chem. Commun.*, 2010, **46**, 2405–2407.
32 J. Halámek, T. K. Tam, S. Chinnapareddy, V. Bocharova and E. Katz, *J. Phys. Chem. Lett.*, 2010, **1**, 973–977.

33 J. B. Zhu, X. Yang, L. B. Zhang, L. L. Zhang, B. H. Lou, S. J. Dong and E. K. Wang, *Chem. Commun.*, 2013, **49**, 5459–5461.
34 X.-J. Jiang and D. K. P. Ng, *Angew. Chem., Int. Ed.*, 2014, **53**, 10481–10484.
35 H. L. Li, W. Hong, S. J. Dong, Y. Q. Liu and E. K. Wang, *ACS Nano*, 2014, **8**, 2796–2803.
36 R. L. Rivest, A. Shamir and L. Adleman, *Commun. ACM*, 1978, **21**, 120–126.
37 B. Rout, P. Milko, M. A. Iron, L. Motiei and D. Margulies, *J. Am. Chem. Soc.*, 2013, **135**, 15330–15333.
38 G. Naren, S. M. Li and J. Andréasson, *ChemPhysChem*, 2017, **18**, 1726–1729.
39 J. Agudelo, V. Privman and J. Halámek, *ChemPhysChem*, 2017, **18**, 1714–1720.
40 M. Bälter, S. M. Li, J. R. Nilsson, J. Andréasson and U. Pischel, *J. Am. Chem. Soc.*, 2013, **135**, 10230–10233.
41 D. Q. Fan, E. K. Wang and S. J. Dong, *Chem. Sci.*, 2017, **8**, 1888–1895.
42 V. Nellore, S. Xi and C. Dwyer, *ACS Nano*, 2015, **9**, 11840–11848.
43 B. Rout, L. Unger, G. Armony, M. A. Iron and D. Margulies, *Angew. Chem., Int. Ed.*, 2012, **51**, 12477–12481.
44 H. B. Sun, S. J. Liu, W. P. Lin, K. Y. Zhang, W. Lv, X. Huang, F. W. Huo, H. R. Yang, G. Jenkins, Q. Zhao and W. Huang, *Nat. Commun.*, 2014, **5**, 3601–3609.
45 D. Y. Tong, H. F. Duan, H. J. Zhuang, J. G. Cao, Z. L. Wei and Y. J. Lin, *RSC Adv.*, 2014, **4**, 5363–5366.
46 S. Shoshani, R. Piran, Y. Arava and E. Keinan, *Angew. Chem., Int. Ed.*, 2012, **51**, 2883–2887.
47 Y. Wu, Y. S. Xie, Q. Zhang, H. Tian, W. H. Zhu and A. D. Q. Li, *Angew. Chem., Int. Ed.*, 2014, **53**, 2090–2094.
48 T. Ratner, O. Reany and E. Keinan, *ChemPhysChem*, 2009, **10**, 3303–3309.
49 G. Strack, H. R. Luckarift, R. Nichols, K. Cozart, E. Katz and G. R. Johnson, *Chem. Commun.*, 2011, **47**, 7662–7664.
50 A. P. de Silva, M. R. James, B. O. F. McKinney, D. A. Pears and S. M. Weir, *Nat. Mater.*, 2006, **5**, 787–790.