# Developing a highly responsive miniaturized security device based on a printed copper ammine energetic composite

Florent Sevely, Tao Wu, Felipe Sodre Ferreira de Sousa, Lionel Séguier, Vincent Brossa, Samuel Charlot, Alain Estève, Carole Rossi

# Developing a highly responsive miniaturized security device based on a printed copper ammine energetic composite

*Florent Sevely, Tao Wu, Felipe Sodre Ferreira de Sousa, Lionel Seguier, Vincent Brossa, Samuel Charlot, Alain Esteve, and Carole Rossi**

LAAS-CNRS, University of Toulouse, 7 Avenue du colonel Roche, 31077 Toulouse, France

*E-mail: rossi@laas.fr

## Highlights

- A novel ultimate security device concept is designed and developed.
- The actuation is based on the pressure generated by the reaction of a confined and safe copper ammine energetic composite placed below the circuitry to be destroyed.
- The pressure burst can be easily tuned by modifying the energetic composite solid loading.
- A fast response is demonstrated.
- The concept and technology hold potential for commercial scale production.

## Abstract

This work presents a triggerable ultimate security device (USD) capable of physically destroying a memory chip that contains classified data within a few milliseconds upon the detection of intrusion. The USD is designed as an add-on module that can be positioned onto any electronic chip, IC circuit, or memory card without requiring any specialized chip design, substrate type or encapsulation solution. Its operation is simply based on the exothermic reaction of a solid-state printed energetic composite that physically disintegrates the sensible component in less than 1 ms. The solid-state energetic composite consists of a mixture of Al/CuO nanothermite with a copper ammine complex densely printed onto the chip that is meant to be destroyed. This energetic layer can be ignited through resistive heating or capacitance discharge in less than 50 µs. The paper details the fabrication and assembly of a test USD device and demonstrates that 400 mg of energetic composite can be used to irreversibly destroy one silicon chip (~120 $mm^3$) in less than 10 ms. The outcome of this work also shows that the reaction time and efficiency are highly dependent on the reactive material loading, i.e., the mass of nanothermites deposited into the device and memory card.

**Keywords:** transient electronics, anti-reverse engineering, anti-hacking, nanoenergetic materials, PyroMEMS, 3D printing

## 1. Introduction

Security has become a vital part of electronic products that are employed in critical data storage (personal, bank, etc.) or critical equipment such as military systems. These electronics not only handle sensitive data in uncontrolled environments but also face intellectual protection issues or counterfeiting issues. Several electronic anti-tamper and anti-reverse engineering technologies exist [1-3]. In brief, the simplest anti-tamping and anti-reverse engineering solutions are based on cryptographic keys or software [4], security fuses or circuit breakers [5] to prevent nonauthorized access, or reinforcement of the component packaging [5, 6] to limit access to sensitive components. More sophisticated solutions, including anti-tamper sensors, are able to detect the type of intrusion, such as Hall-effect switches [7]. Often, several different anti-tamper protections are integrated to ensure efficient protection [8].

Unfortunately, all current anti-tamping technologies, while being effective and in constant evolution to adapt to new complex topologies and progressing technologies, are susceptible to being cracked or bypassed, leaving the system vulnerable. That is why an ultimate action must be considered upon the detection of intrusion based on irreversible destruction of the component being attacked. Indeed, irreversibly destroying the component and its stored data is the most secure and cost-effective way to dispose of sensitive information such as topology, access code or private data. From this viewpoint, the use of transient electronic devices [9, 10] was explored to destroy the sensitive component based on various mechanisms, such as light, heat, or mechanical impact. However, the transience technology is mostly too slow, taking several minutes to a few days to act. It also imposes several a priori restrictions in terms of chip design and materials, making it unsuitable for the semiconductor industry at large. Alternative works have explored the release of acids or corrosives [11] to chemically degrade an electronic chip. Another study has explored a transient mechanism based on the distribution of thermally actuating material [12] within the silicon chip to fracture it under the stress generated. While each of these methods succeeded in either mechanically or chemically destroying the silicon chip, they present severe limitations on the time scale needed to achieve destruction (minutes), on the input energy required to render the device totally inoperable and on required restrictions in term of chip design. Other alternative works

have considered the heat generated by the exothermic reaction of an energetic material to mechanically destroy an electronic device [8, 13-15]. A few milligrams of energetic layers, such as Al/$Bi_2O_3$ nanothermites, were found to be effective in fracturing silicon wafers, whereas the same amount of Al/CuO failed [8]. In [13], a thick nanothermite-based film (Al/CuO powder mixed with gasoline and benzene) was spin coated on top of a microchip during the microfabrication steps. Authors observed the effect of thermite-enabled destruction prior to and after ignition through microscopic imaging and electrical measurements. This work provides conclusive evidence that when ignited, the thermite layer releases enough heat to melt the surface and damage the surface bound components within 1 s, much shorter than the time required for thermally actuated mechanisms, but fails to confirm the irreversible destruction of data contained in the bulk. In a very recent work [15] graphene oxide-energetic coordination polymer energetic composite was used to demonstrate a transient microchip device. Authors demonstrate the destruction of the chip within one second.

The key objective of this research is to develop and test a modular, highly responsive, safe (no sensitive material such as Al/$Bi_2O_3$) device that acts as an add-on module that can be placed on any IC (integrated circuit) circuit, off-the-shell component, or memory card without requiring any specialized chip design, substrate type or encapsulation solution. This so-called ultimate security device (USD) compatible with an embedded system environment can be actuated in less than 100 microseconds to mechanically disintegrate any types of components containing sensible data upon the detection of intrusion into the system. The actuation mechanism is provided by using a printed copper ammine complex-based energetic composite [16-17]; this material was chosen as it is a source of reliable, safe and “dormant” energy, exhibiting a long shelf life (decades) and able to very quickly deliver gas and heat through a self-sustained redox reaction. Whereas the Al/CuO thermite generates a very limited amount of gas, the addition of copper ammine complex greatly enhances the pressurization rate and gas generation so that to better achieve the component destruction.

Previous studies have demonstrated the capabilities of nanothermite-based energetic films to provide high-energy density actuations to fracture silicon substrates [18] or disconnect circuitry [19] while being safe and stable until 250 °C [20-22], but none have demonstrated the irreversible destruction of data contained in the bulk silicon memory. Herein, we specifically design and elaborate a printable copper ammine complex-nanothermite composite featuring a higher pressurization capability than nanothermite powder to produce

fast and highly efficient mechanical actuation. The paper is organized as follows: Section 2 presents the USD concept, operation principle and design. Section 3 describes the thermite-based energetic composite synthesis and printing and the fabrication of each layer of the USD. Finally, Section 4 presents an ensemble of miniaturized USD test demonstrators (~9.5 $cm^3$) with varying energetic mass loading mounted onto a SD memory card. Tests demonstrate the irreversible physical destruction of the silicon chip, and, thus, all readable data in the memory for an energetic composite mass of greater than 300 mg.

## 2. USD operation principle and design

The USD operates autonomously in response to an order-related signal received from a control unit, as illustrated in [13]. Upon the detection of an intrusion, the control unit sends a key code. If the code does correspond to the trigger logic for the activation of the USD operation, the control unit activates the USD initiation through an electrical command signal sent to the initiation module, which then triggers the charging of a capacitor connected to a power supply (power unit) followed by its discharge to the USD initiator that triggers the energetic composite reaction, leading to the destruction process.

The methods used to implement hardware protection using key-based obfuscation have already been developed and well documented in the literature [23, 24]. That is why in this paper, we will focus on the novel aspects, *USD initiation unit* and *destruction mechanisms*.

The main active part of the USD, i.e., to realize the initiation and chip destruction consists of multiple successive layers, as represented in the schematic diagram shown in **Figure 1a**:

- The nanothermite/copper ammine-based energetic composite is ink-printed onto the device for protection. The mass of the deposited composite varies from 100 to 600 mg as a function of the energy required for the irreversible destruction of the component. Details for the elaboration and deposition of the energetic nanocomposite are given in Section 3.
- The initiation circuitry integrates a pyroMEMS [25-28] to trigger the reactive composite combustion upon electronic order. The pyroMEMS consists of a stack of 15 Al/CuO bilayers deposited [26] onto a thin-film resistive filament. When a current is applied to the resistive filament, the Al/CuO reactive film is ignited by the Joule effect and reacts to produce a flame. Because pyroMEMS is manufactured using microelectronic manufacturing techniques (cf. Section 3), it can be easily

interconnected with electronics, which enables control of the entire ignition process, as detailed in Section 2.1.

The operational principle of the device is depicted in **Figure 1**. The USD is positioned onto the sensitive component to be secured (**Figure 1** (2)) and can remain in sleeping mode for years until a threat is detected; once detected and confirmed (**Figure 1** (3)), the pyroMEMS is ignited in less than 100 µs and further ignites the energetic composite (**Figure 1** (4)). Its combustion generates a heat and pressure impulse that bursts the target component (**Figure 1** (5)).

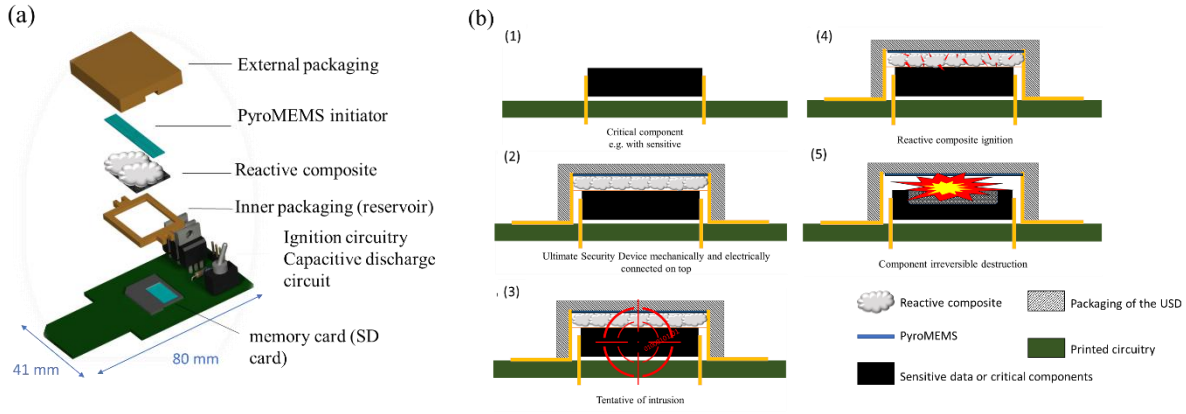


***Figure 1.*** *Conceptual illustration of the USD operation principle: (a) exploded view of an USD device composed of 2 stacked parts: the initiation circuitry with a pyroMEMS and the copper ammine/nanothermite-based energetic composite printed in a reservoir (inner packaging). (b) Illustration of the different steps of operation, from the detection to the destruction mechanisms.*

## 2.1. Initiation unit design

Requirements for the initiation circuit are as follows: the pyroMEMS must be ignited with the lowest possible energy and in less than 100 µs. However, pyroMEMS must be totally safe. This latter requirement means that during the possibly long lifetime of the component operation under normal conditions, the risk of undesired ignition must be null. We have chosen to ignite the pyroMEMS through a capacitive discharge using a 10 µF capacitor (maximum voltage of 15 VDC) for its ease of integration into the electronic circuitry. Thus, the circuitry includes charge and discharge switches **(Figure 2a)**. We use 3 MOS transistors: one NMOSFET for the discharge and one NMOSFET driven by a PMOSFET for the charging of the capacitor (**Figure 2b**). The trigger signal sent by the control unit opens the charge MOSFET, and another signal is sent to close the discharge MOSFET, enabling the capacitor to discharge in the pyroMEMS resistive filament (5 Ω) to trigger the energetic

composite reaction. Depending on the application requirements, it is also possible to maintain the capacitor in a continuously charge state, which means that the charging switch must be kept closed to keep the capacitor always connected to the power supply. This solution reduces the USD response time by 10 µs (the time needed for charging the capacitor), but at the cost of increased energy consumption to compensate for the current leakage through both transistors and capacitors.

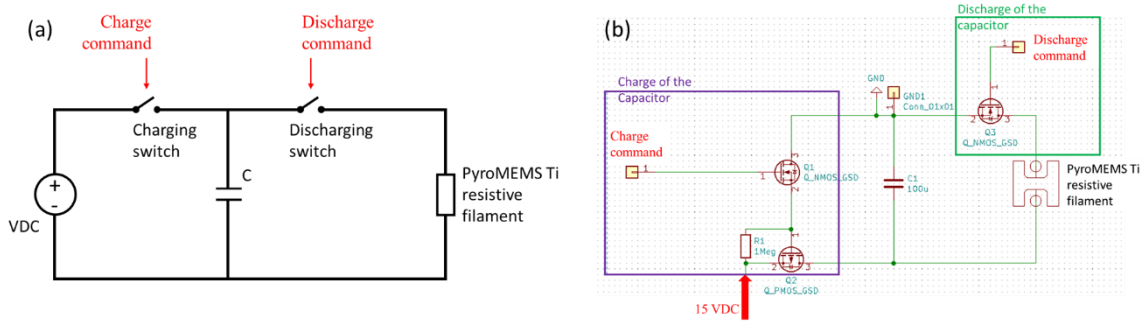


***Figure 2.*** *Design of the initiation unit: (a) schematic of the capacitive discharge circuit and (b) electronic circuitry with the discharge transistor (NMOSFET) shown in green and the charge transistors (NMOSFET + PMOSFET) shown in purple.*

The actual pyroMEMS used in this prototype has a 100% rate ignition success at 15 V. To be compatible with embedded systems, it was implemented with a capacitive discharge circuit, and a tension boost circuit using a *LT3580 Linear technology DC/DC boost*. The boost component was polarized to raise the input voltage from 5 V to 15 V. Despite this light implementation, we were still able to charge our capacitor to 15 V and maintain a 100% pyroMEMS ignition success rate. For our preliminary tests, a simplified version of the initiation circuitry was considered using only the capacitive discharge circuit powered by a 15 V lab. power supply. The circuitry was mounted onto the main PCB, as shown in **Figure 6b**. Inside the box, only a pyroMEMS with long connection pads was present, and the connection between the main PCB and the pyroMEMS was made via two holes in the box, leaving the pyroMEMS pads apparent.

## 3. Fabrication and assembly

The successive layers, e.g., the PyroMEMS, the energetic composite and the reservoir, were designed, fabricated as detailed in this section before being assembled and mounted onto the memory or component to be destroyed.

### 3.1. PyroMEMS fabrication

A 500-µm thick 4-inch glass substrate was cleaned with oxygen plasma at 800 W for 5 min to remove surface contamination. Next, negative nLof photoresist (AZ nLof 2035, MicroChem Corporation, USA) was spin-coated and patterned using photolithography. Subsequently, 350-nm-thick titanium and 300-nm-thick gold layers were evaporated onto the surface, and then a second photolithography step with positive photoresist was performed to define the Ti resistive filament and Au electrical pads by chemical etching of the gold. Finally, an ~13 mm² stack of 15 Al/CuO bilayers (~300 nm thick) was sputter deposited as described in [25-28] directly in contact with the Ti electrical resistance. The main process steps are summarized in **Figure 3**.

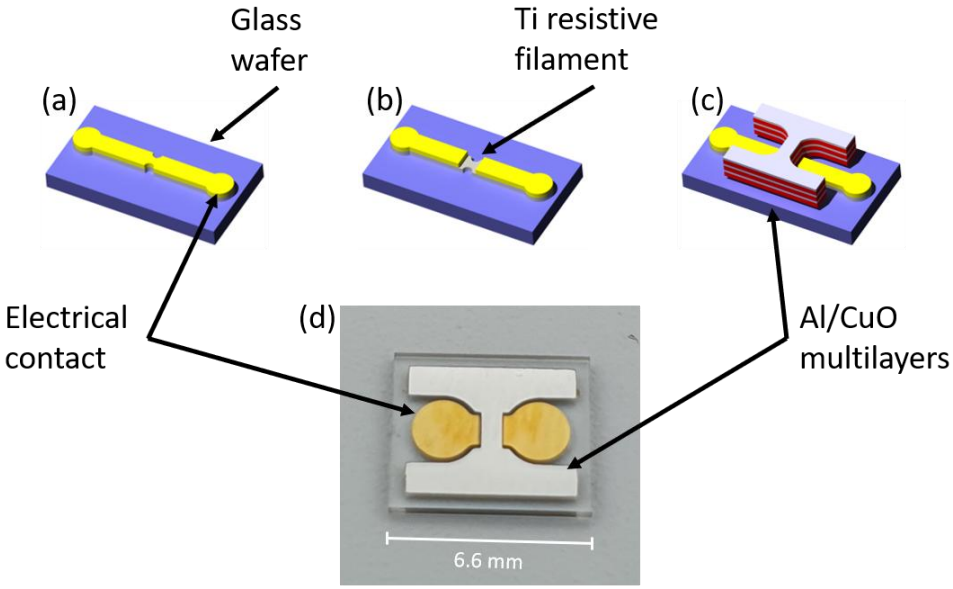


***Figure 3.*** *3D schematic views of the main pyroMEMS fabrication steps: (a) Ti and Au deposition on a glass wafer, (b) etching of Au to define the electrical tracks and Ti resistance, (c) sputter-deposition of the Al/CuO multilayered reactive film, and (d) real view snapshot.*

### 3.2. Energetic composite preparation and deposition

The aluminum nanopowders (Al, average particle size: 80 nm, purity: 69%) were purchased from Novacentrix (USA) and stored in a glove box before use. Copper oxide (CuO, average particle size: 100 nm), copper nitrate trihydrate, 25% aqueous ammonia, ethanol ($CH_3CH_2OH$, anhydrous, 99.9%), and polyvinylpyrrolidone (PVP, molar weight: 40k) purchased from Merck (Germany) were directly used as received. To prepare Al/CuO nanothermites, 456 mg of Al powder and 1 017 mg of CuO were dispersed in ethanol and then stirred for 45 minutes in a sonication bath cooled by ice. The suspension was then dried at 50 °C. The dry powder

(referred to as Al/CuO) was collected and reserved for future use. Note that the masses of Al and CuO were calculated based on an equivalence ratio of 1.2.

The copper ammine complex (CuC), $Cu(NH_3)_4(NO_3)_2$, was synthesized and cryo-milled to reduce its size, as detailed in [17]. In brief, 4.83 g (0.02 mol) of copper nitrate trihydrate was dissolved in 10 mL of distilled water followed by the addition of 15 mL of 25% aqueous ammonia solution (0.24 mol). The final product (micron-sized powder) was separated via vacuum filtration and dried in an oven (Carbolite Gero, England) at 70 °C. The as-synthesized CuC powders were milled using a Retsch CryoMill machine using $ZrO_3$ grinding balls (diameter: 2.5 mm). The milling parameters were as follows: frequency of 30 Hz (30/s) for 10 min while subject to liquid-$N_2$ cooling.

Then, 1473 mg of Al/CuO was mixed with 427 mg of milled CuC powder to produce energetic nanocomposites, referred to as Al/CuO/CuC. The exothermic self-sustained reaction of Al/CuO/CuC occurs via several steps upon heating:

At 270 °C:

$$2Cu(NH_3)_4(NO_3)_2(s) \rightarrow 2CuO(s) + 9H_2O(g) + 2NH_3(g) + 4N_2(g) + N_2O(g)$$

At 575 °C:

$$2\ CuO\ (s) \rightarrow 1/2\ O_2\ +\ Cu_2O(s)$$

At 780 °C:

$$2Al\ (s) + 3Cu_2O\ (s) \rightarrow Al_2O_3(s) + 6Cu(s)$$

The equivalence ratio for the CuC over Al/CuO nanopowder was 25%, which was chosen to obtain the highest pressure burst and burn rate (see ref [16]). Notably, the combustion speed under unconfined conditions was characterized by a high-speed camera at ~ 141 $m.s^{-1}$.

The next step consists in preparing the energetic ink to be deposited by printing into the USD reservoir. For that purpose, 2 g of Al/CuO/CuC was dispersed with 100 mg (5% wt) of the binding polymer polyvinylpyrrolidone (PVP, average molecular weight 40 000 g $mol^{-1}$ purchased from *Sigma–Aldrich*) in ethanol (4 ml) and then stirred for 2 hours in a sonication bath cooled by ice. With 5% wt of PVP, the energetic ink is homogeneous and stable for at least 24 h, enabling reproducible and semiautomatic deposition. The deposition time for 400 mg of Al/CuO/CuC ink is ~1 h using the semiautonomous deposition machine (**Figure 4b**).

This polymer-coated Al/CuO/CuC ink is relatively compact with a final thin film characterized by a density of 65% of its theoretical maximum density, TMD (see **Equation 1**). It should be noted that without PVP binding, the maximum achievable compaction is close to 45% TMD. However, as a counterpart, being a nonenergetic binder, adding 5% wt PVP with Al/CuO/CuC alters the energetic performance: the combustion speed is reduced by ~80%, i.e., 17 $m.s^{-1}$ for Al/CuO/CuC +5% wt PVP against 141 m/s without PVP, as detailed in [29].

**Figure 4a** summarizes the preparation steps for the energetic composite, and **Figure 4b** shows the deposition bench specifically developed to deposit the ink into the USD reservoir. It is composed of a homemade 3D printer with a 3-axis controller, a syringe driver (composed of a stepper motor, a 3D printed structure in PolyLactic Acid & a 5 ml syringe) controlled by an *Arduino card* and supervised by a LabVIEW program. The ink deposition is first calibrated and then controlled using the motor step. The precision of the deposition is ± 5%, i.e., ± 5 mg for the deposition of 100 mg. **Figure 4c** gives snapshot images of the energetic ink in the vial with a zoom (electron microscopy images) of the dried ink after deposition. After drying, the density of the printed material reaches 2.3 $g/cm^3$ i.e., 65 %TMD.

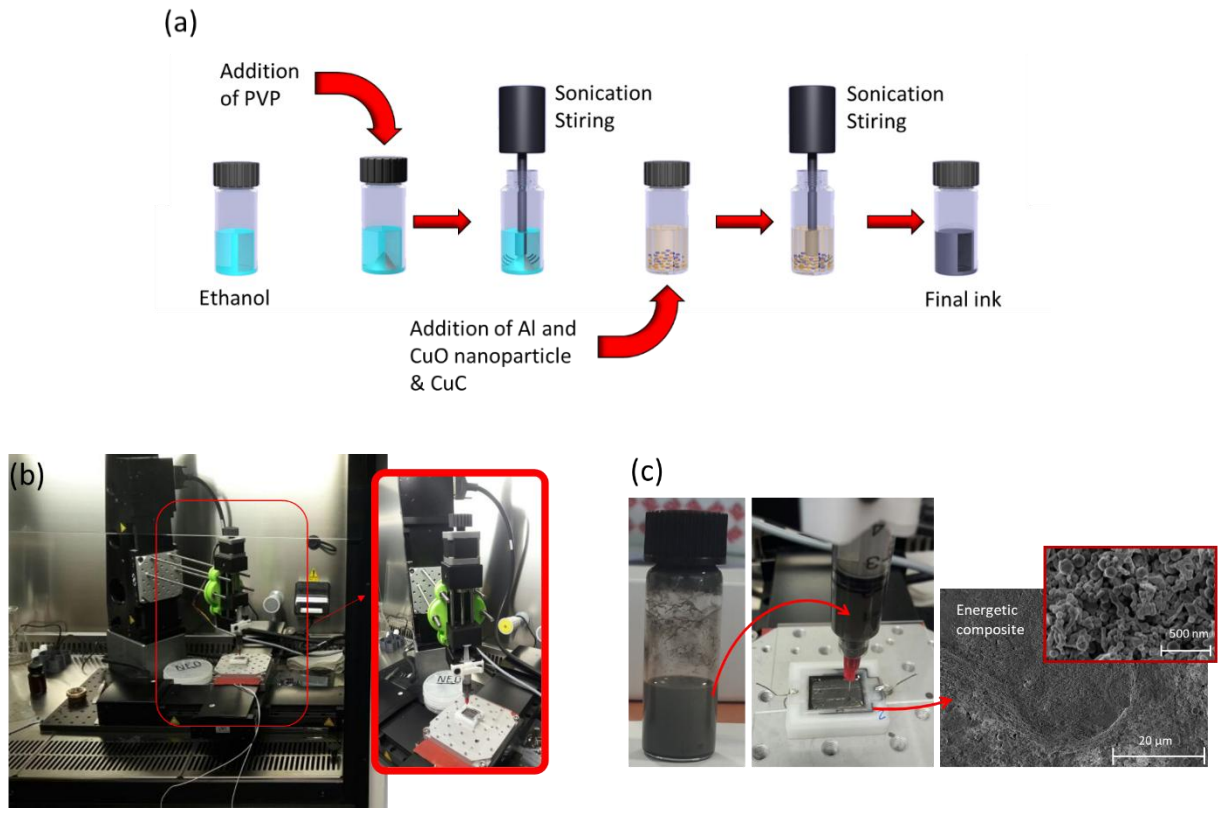

***Figure 4**. Energetic ink preparation and deposition: (a) schematic of the copper ammine complex and nanothermite ink preparation. (b) Photograph of the homemade 3D printer with the syringe driver pushing the syringe filled with energetic ink and the 3-axis controller.*

### 3.3. Reservoir and external packaging fabrication

The USD packaging consists of two parts:

1. The external packaging (brown piece in **Figure 5a**) is a rectangular cap.
2. A rectangular reservoir (violet piece in **Figure 5a**) designed to fit the dimension of the chip to be protected (SD memory for demonstrator) with two functions: block the pyroMEMS in its trench and store the energetic composite. The initiation circuitry is inserted between the external packaging and the rectangular reservoir, as illustrated in **Figures 5a- b.**

On both sides of the packaging, holes permit electrical connections of the initiation circuitry with the printed board circuitry containing the target component, as described in the next section.

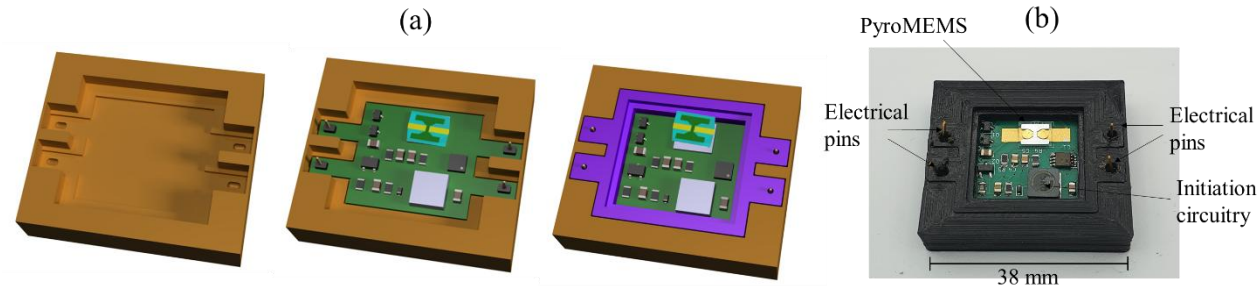


***Figure 5.** The USD packaging: (a) schematic of the 3 main parts of the USD with the external packaging in brown, the pyroMEMS in blue, the reservoir in which the energetic composite is printed in purple, and (b) a photo of the reservoir with the initiation circuit inside.*

Both parts were 3D printed in Nylon (*Nylon, Ultimaker, Netherlands*) using a 3D printer (*Ultimaker S5*), as shown in **Figure 5b**. 3D printing technology was chosen because it offers a good resolution (± 6.9 µm) while being low cost and fast for prototyping a custom-made device. In addition, nylon offers a good compromise between cost and thermal and mechanical resistance (**Table 1**).

***Table 1.** Main physical and thermal characteristics of the nylon used to fabricate the packaging and reservoir. https://ultimaker.com/materials/nylon*

| Tensile modulus | Tensile stress at yield | Tensile stress at break | Flexural strength | Flexural modulus | Izod impact strength | Melting temperature |
|---|---|---|---|---|---|---|

| | | | | | | |
|---|---|---|---|---|---|---|
| 579 MPa | 27.8 MPa | 34.4 MPa | 24 MPa | 463.5 MPa | 34.4 KJ/$m^2$ | 185 °C |

## 4. Test device assembly and tests

Ten USD demonstrators were designed and fabricated to validate the concept. An off-the-shelf SD memory card (*Transcend SDHC memory Card 8GB, Taiwan)* was chosen as the component to be destroyed for the demonstration tests. It offers the advantage of being easily readable and programmable with a computer. Its packaging is composed of 500 µm thick epoxy resin reinforced with microsilica balls and fireproof composite, making it resistant to heat and pressure. Therefore, we first chemically etch the packaging to open an ~5 × 10 $mm^2$ squared window into the packaging to access the silicon microchip (**Figure 6a**), taking care to not damage the internal wire bonding and electrical connections or the passive components and the silicon chip that constitute the memory. The prepared SD card is then checked, programmed, mounted and connected to the printed board circuitry (PCB) serving for the test, as shown in **Figure 6b**. A simplified initiation unit and PCB designed with a USB drive shape are used to demonstrate the destruction of the SD card. One side of the PCB contains the charging and discharging switches with the initiation trigger switch simulating the electrical signal sent by the order unit upon intrusion detection. The SD card is glued onto the PCB, and its contact pads are attached onto the back side of the PCB, enabling the SD to be connected to a computer.

In parallel, a mass of energetic composite ranging from 100 mg to 600 mg is printed into the nylon reservoir (volume of 268 $mm^3$) containing one pyroMEMS and sealed with a cellophane thin film (**Figure 7c**). Then, the external packaging (in brown in **Figure 5a**) is glued on the main PCB using a bi-component epoxy glue (3M Scotch-Weld Epoxy Adhesive 2216) which permits to keep the mechanical integrity of the USD assembly during the operation. The final step involves the electrical connection of the pyroMEMS electrical pads with the initiation circuitry electrical connections.

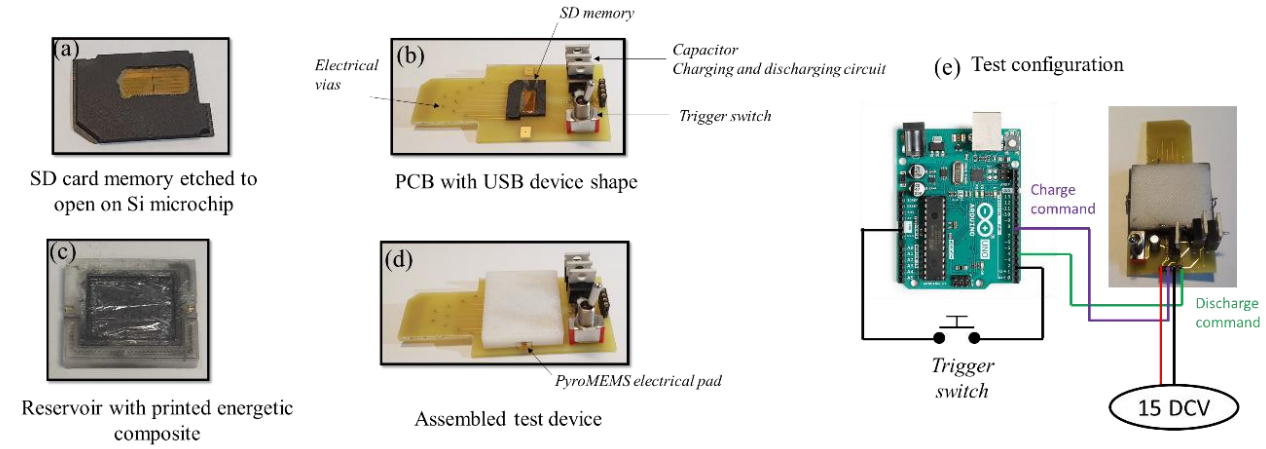


***Figure 6.*** *Photographs of (a) the SD card after being locally etched to reveal the silicon microchip that stores the sensible data, (b) the prepared SD card glued onto the demo PCB featuring a simple capacitive discharge circuit, (c) reservoir with printed energetic composite, (d) an assembled test device for demonstration tests, and (e) schematic of the demonstration test configuration.*

### 4.1. Initiation procedure and conditions

For the destruction tests, the initiation of the pyroMEMS (**Figure 6e**) is powered by a laboratory power supply at 15 VDC and driven by an *Arduino prototyping board* connected to the PCB. The intrusion is simulated by a push button (trigger switch of **Figure 6b**) providing the trigger electrical signal to the Arduino card, which then successively sends two square signals with a duration of 100 µs spaced by 10 µs to the charge and discharge pins to charge the capacitor and to discharge it into the resistive filament of the pyroMEMS. The initiation steps are illustrated in **Figure 7a**, presenting the sequence of electrical signals leading to the initiation of the pyroMEMS (photograph in **Figure 7b**). We measured a duration time of 168 µs between the order and pyroMEMS initiation. The 10 µF capacitor charges to its maximum voltage in 30 µs, and pyroMEMS ignites within 24 µs upon ignition.

After removing the excess time to full charge of the capacitor (70 µs) and time before each signal (13 µs) (**supporting information Figure S1 and S2**), the minimum USD reaction time after an intrusion is detected and confirmed by the control unit is only ~85 µs.

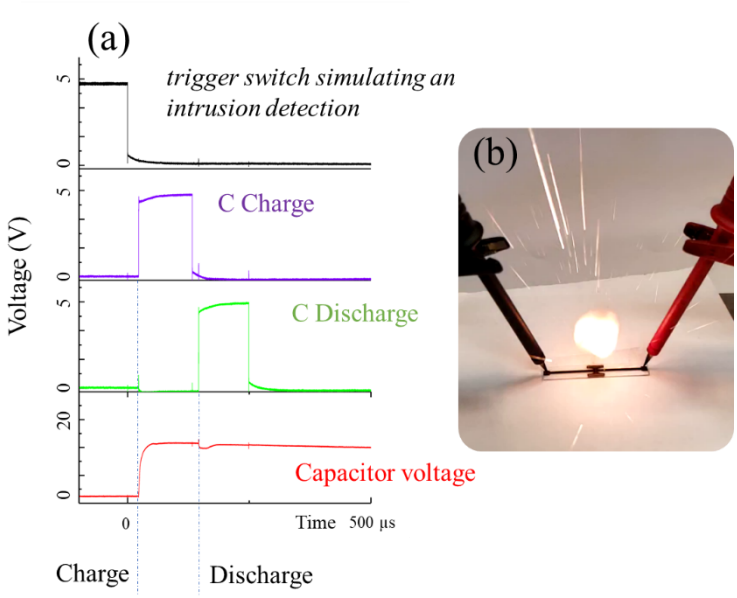


***Figure 7.*** *Ignition characterization: (a) electrical command sequence and capacitor discharge. (b) Photograph of the reaction of one pyroMEMS.*

### 4.2. Destruction tests

Height demonstrators similar to those shown in **Figure 6d** were assembled with different masses of energetic composites varying from 13 mg to 600 mg, corresponding to different compaction rates expressed in percentage of the TMD (noted %TMD, **Equation 1**): 13 mg (%TMD 45%) and 100 mg (%TMD 11%) to 600 mg (%TMD 64%).

$$\%\text{TMD} = \frac{\text{mass of reactive composite}}{\text{TMD} \times \text{volume of the reservoir}} \times 100 \qquad (1)$$

where TMD is the theoretical maximum density of the reactive composite, equal to 3.51 g/cm$^3$ for our Al/CuO/CuC composition. The volume of the reservoir is 268 mm$^3$.

For each mass, 3 tests were performed. After the ignition and combustion of the copper ammine complex-based energetic composite, the demonstrators are opened, and SD cards are observed visually using a Microscope *Hirox RX-100* with ×20 and ×140 magnification. Pictures were taken using a multifocus technique enabling us to observe rifts/trenches in a fully reconstituted 3D picture. The results are summarized in **Figure 8** for configurations with energetic composite masses of 200 mg (a), 300 mg (b), 400 mg (c) and 600 mg (d). Each demonstrator was ignited following the procedure detailed in subsection 4.1. Finally, the USD was disassembled to characterize the state of the chip. The results are given as snapshot images of the SD cards after the tests: (i) non-magnified, (ii) ×20 magnification, (iii) and (iv) ×140 magnification.

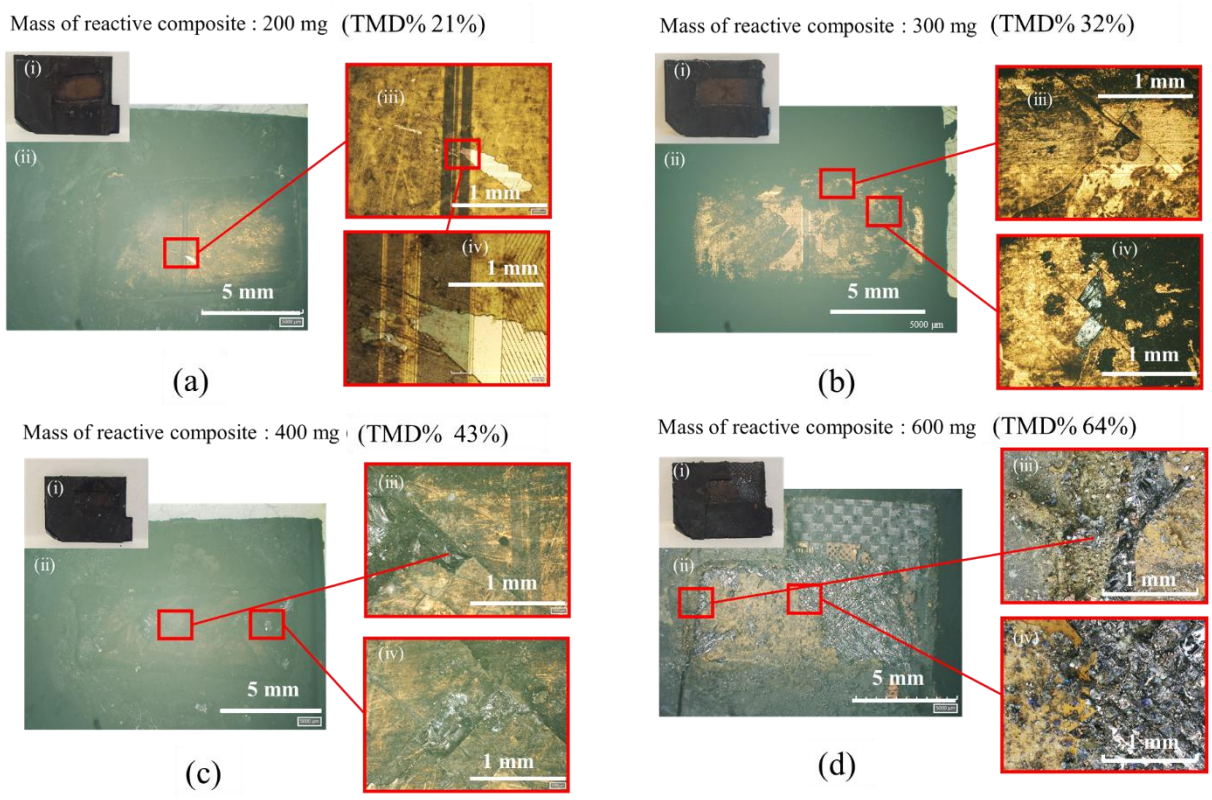


***Figure 8.*** *Photographs of SD cards after tests with energetic composite masses of (a) 200 mg or 90 mm$^3$, (b) 300 mg or 130 mm$^3$ (c) 400 mg or 170 mm$^3$ (d) 600 mg or 268 mm $^3$ and with their insert (i) a global photograph of the SD card, (ii) microscope imaging with ×20 magnification and (iii/iv) microscope imaging with ×140 magnification.*

We observe that with a 600 mg load of energetic composite, the SD card is totally destroyed: a part of the packaging is torn out, and most of the silicon chip is disintegrated. When not disintegrated, the silicon features rifts and holes (**Figure 8d** (iii) and (iv)). With 400 mg loading, some parts of the silicon chip are disintegrated, and rifts run across the chip. Although the damage is less intense compared to the case of a 600 mg reactive composite, the SD is sufficiently damaged to guarantee total destruction of the data. With 300 mg, some cracks appear on the silicon chip, and some shards are torn off (**Figure 8b** (iii) and (iv)). The silicon surface is covered by a superficial scratch, but the silicon chip remains unbroken as well as the data. With a less reactive composite, i.e., < 200 mg in mass, the silicon surface remains completely intact. The reaction damages only the wire bonding.

These results validate the good functioning of our USD module, as we can destroy the silicon component with all the data in it for an energetic composite mass of greater than 400 mg in less than 1 ms.

## 5 Conclusion

This work reports the successful implementation of a triggerable, modular and fast ultimate security device capable of destroying a silicon chip containing sensible data in tens of milliseconds. making the data completely unreadable. This destruction is possible thanks to the highly exothermic reaction of a solid-state energetic composite composed of a mixture of Al/CuO nanothermite with an ammine copper complex densely printed onto the chip to be protected. This energetic layer is ignited by capacitance discharge in less than 100 µs. We demonstrate that 400 mg of energetic composite enables irreversible destruction of one silicon chip (~118 $mm^3$) in less than 10 ms. The outcome of this work also outlines the fact that the reaction time and efficiency are highly dependent on the energetic composite loading, i.e., the mass of CuC/nanothermite printed into the device in contact with the memory card. Importantly, this ultimate security device is a versatile solution that can be implemented for any tunable mechanical actions for release, severance/fracture, jettison, switching, time delay, and actuation. Therefore, it can be successfully implemented for multiple relevant emergency safety responses, which clearly responds to the crucial need to fight against data theft and reverse engineering.


## Acknowledgements

The authors acknowledge support from the European Research Council (H2020 Excellent Science) Researcher Award (grant 832889 – PyroSafe). This work was also supported by LAAS-CNRS technology platform, a member of Renatech network. We acknowledge the French Defense Agency which partially funds F.S. scholarship. The authors also acknowledge the help from Pierre Burgaud and Julien Nicolod in opening commercial SD memories packaging.


## References


[1] I. McLoughlin, Secure embedded systems: the threat of reverse engineering, Proceedings of the 14th IEEE Trans Parallel Distrib Syst (2008), 729-736, https://doi.org/10.1109/Icpads.2008.126.

[2] E. Burd, M. Munro, Using evolution to evaluate reverse engineering technologies: mapping the process of software change, J Syst Softw 53 (1) (2000), 43-51, https://doi.org/10.1016/S0164-1212(00)00007-8.

[3] Z. Guo, M. Tehranipoor, D. Forte, J. Di, Investigation of Obfuscation-based Anti-Reverse Engineering for Printed Circuit Boards, 2015 52nd Acm/Edac/IEEE Design Automation Conference (Dac) (2015), https://doi.org/10.1145/2744769.2744862.

[4] J. Park, Y. Park, Symmetric-Key Cryptographic Routine Detection in Anti-Reverse Engineered Binaries Using Hardware Tracing, Electronics 9 (6) (2020), 957, https://doi.org/10.3390/electronics9060957.

[5] A. R. Desai, D. Ganta, M. S. Hsiao, L. Nazhandali, C. Wang, S. Hall, Anti-counterfeit Integrated Circuits Using Fuse and Tamper-Resistant Time-stamp Circuitry, IEEE International Conference on Technologies for Homeland Security (Hst) (2013), 480-485.

[6] L. W. Li, P. J. Wang, Y. J. Zhang, Design of anti-key leakage camouflage gate circuit for reverse engineering based on dummy vias, Microelectron. J. 90 (2019), 163-168, https://doi.org/10.1016/j.mejo.2019.06.006.

[7] S. Patnaik, N. Rangarajan, J. Knechtel, O. Sinanoglu, S. Rakheja, Advancing Hardware Security Using Polymorphic and Stochastic Spin-Hall Effect Devices, Design Automation and Test in Europe (2018), 97-102.

[8] T. J. Fleck, R. Ramachandran, A. K. Murray, W. A. Novotny, G. T. C. Chiu, I. E. Gunduz, S. F. Son, J. F. Rhoads, Controlled Substrate Destruction Using Nanothermite, Propellants Explos. Pyrotech. 42 (6) (2017), 579-584, https://doi.org/10.1002/prep.201700008.

[9] C. H. Cheng, D. S. Yang, J. Kim, P. B. Deotare, Self-erasable and rewritable photonic platform for antitamper hardware, IEEE Photon. Conf. (2020).

[10] S. S. Pandey, C. H. Mastrangelo, Towards Transient Electronics through Heat Triggered Shattering of Off-the-Shelf Electronic Chips, Micromachines (Basel) 13 (2) (2022), 242, https://doi.org/10.3390/mi13020242 .

[11] C. W. Park, S. K. Kang, H. L. Hernandez, J. A. Kaitz, D. S. Wie, J. Shin, O. P. Lee, N. R. Sottos, J. S. Moore, J. A. Rogers, S. R. White, Thermally Triggered Degradation of Transient Electronic Devices, Adv. Mater. 27 (25) (2015), 3783-3788, https://doi.org/10.1002/adma.201501180.

[12] N. Banerjee, Y. Xie, M. M. Rahman, H. Kim, C. H. Mastrangelo, From Chips to Dust: The Mems Shatter Secure Chip, IEEE 27th International Conference on Micro Electro Mechanical Systems (MEMS) (2014), 1123-1126.

[13] S. S. Pandey, C. H. Mastrangelo, An Exothermal Energy Release Layer for Microchip Transience, IEEE Sens. J. (2013), 1759-1762, https://doi.org/10.1109/ICSENS.2013.6688572.

[14] S. S. Pandey, N. Banerjee, Y. Xie, C. H. Mastrangelo, Self-Destructing Secured Microchips by On-Chip Triggered Energetic and Corrosive Attacks for Transient Electronics, Adv. Mater. Technol. 3 (7) (2018), 1800044, https://doi.org/10.1002/admt.201800044.

[15] X. Ma, S. Gu, Y. Li, J. Lu, G. Yang, K. Zhang, Additive-Free Energetic Film Based on Graphene Oxide and Nanoscale Energetic Coordination Polymer for Transient Microchip, Adv. Funct. Mater., 2103199 (2021), https://doi.org/10.1002/adfm.202103199.

[16] T. Wu, F. Sevely, B. Julien, F. Sodre, J. Cure, C. Tenailleau, A. Esteve, C. Rossi, New coordination complexes-based gas-generating energetic composites, Combust Flame 219 (2020), 478-487, https://doi.org/10.1016/j.combustflame.2020.05.022.

[17] T. Wu, F. Sevely, S. Pelloquin, S. Assie-Souleille, A. Esteve, C. Rossi, Enhanced Reactivity of Copper Complex-Based Reactive Materials via Mechanical Milling, Combust Flame 233 (2021), 111598, https://doi.org/10.1016/j.combustflame.2021.111598.

[18] L. Glavier, A. Nicollet, F. Jouot, B. Martin, J. Barberon, L. Renaud, C. Rossi, Nanothermite/RDX-Based Miniature Device for Impact Ignition of High Explosives, Propellants Explos. Pyrotech. 42 (3) (2017), 307-316, https://doi.org/10.1002/prep.201600154.

[19] A. Nicollet, L. Salvagnac, V. Baijot, A. Estève, C. Rossi, Fast circuit breaker based on integration of Al/CuO nanothermites, Sens Act A: Physical, 273 (2018), 249-255, https://doi.org/10.1016/j.sna.2018.02.044.

[20] A. Esteve, G. Lahiner, B. Julien, S. Vivies, N. Richard, C. Rossi, How Thermal Aging Affects Ignition and Combustion Properties of Reactive Al/CuO Nanolaminates: A Joint Theoretical/Experimental Study, Nanomaterials (Basel) 10 (10) (2020), 2087, https://doi.org/10.3390/nano10102087.

[21] T. Wu, G. Lahiner, C. Tenailleau, B. Reig, T. Hungria, A. Esteve, C. Rossi, Unexpected Enhanced Reactivity of Aluminized Nanothermites by Accelerated Aging, Chem. Eng. J. 418 (2021), 129432, https://doi.org/10.1016/j.cej.2021.129432.

[22] I. Abdallah, J. Zapata, G. Lahiner, B. Warot-Fonrose, J. Cure, Y. Chabal, A. Esteve, C. Rossi, Structure and Chemical Characterization at the Atomic Level of Reactions in Al/CuO Multilayers, ACS Appl. Energy Mater. 1 (4) (2018), 1762–1770, https://doi.org/10.1021/acsaem.8b00296.

[23] R. S. Chakraborty, S. Bhunia, HARPOON: An Obfuscation-Based SoC Design Methodology for Hardware Protection, IEEE Trans. Comput. Aided Design 28 (10) (2009), 1493-1502, https://doi.org/10.1109/TCAD.2009.2028166.

[24] R. S. Chakraborty, S. Bhunia, Security Against Hardware Trojan Attacks Using Key-Based Design Obfuscation, J. Electron. Test 27 (6) (2011), 767-785, https://doi.org/10.1007/s10836-011-5255-2.

[25] L. Salvagnac, S. Assie-Souleille, C. Rossi, Layered Al/CuO Thin Films for Tunable Ignition and Actuations, Nanomaterials (Basel), 10 (10) (2020), 2009, https://doi.org/10.3390/nano10102009.

[26] C. Rossi, Engineering of Al/CuO Reactive Multilayer Thin Films for Tunable Initiation and Actuation, Propellants Explos. Pyrotech. 44 (1) (2019), 94-108, https://doi.org/10.1002/prep.201800045.

[27] J. L. Pouchairet, C. Rossi, PyroMEMS as Future Technological Building Blocks for Advanced Microenergetic Systems, Micromachines (Basel), 12 (2) (2021), 118, https://doi.org/10.3390/mi12020118.

[28] J. Zapata, A. Nicollet, B. Julien, G. Lahiner, A. Esteve, C. Rossi, Self-propagating combustion of sputter-deposited Al/CuO nanolaminates, Combust Flame, 205 (2019), 389-396, https://doi.org/10.1016/j.combustflame.2019.04.031.

[29] F. Sevely, X. W. Liu, T. Wu, F. Mesnilgrente, B. Franc, S. Assie-Souleille, X. Dollat, C. Rossi, Effect of Process Parameters on the Properties of Direct Written Gas-Generating Reactive Layers, ACS Appl. Polym. Mater. 3 (8) (2021), 3972-3980, https://doi.org/10.1021/acsapm.1c00513.

**TOC**