

Article

Smartphone-Readable Time Response-Encoded Phosphorescent Labels and Authentication Protocols for Internet of Things Applications

Yaovi Ahadjitse ¹, Kristian Nikolov ², Tinko Eftimov ^{1,2,*} , Virginija Vitola ³ , Katrina Krizmane ³ and Awa Sow ¹

¹ Centre de Recherche en Photonique, Université du Québec en Outaouais, 101 Rue St-Jean Bosco, Gatineau, QC J8Y 3G5, Canada; ahay01@uqo.ca (Y.A.); sowa61@uqo.ca (A.S.)

² Central Laboratory for Applied Physics, Bulgarian Academy of Sciences, 61 Blvd Sanct Peterburg, 4000 Plovdiv, Bulgaria; kristian.nikolov@clapbas.bg

³ Institute of Solid State Physics, University of Latvia, Ķengaraga Iela 8, Latgales Priekšpilsēta, LV-1063 Riga, Latvia; virginija.vitola@cfi.lu.lv (V.V.); katrina.krizmane@cfi.lu.lv (K.K.)

* Correspondence: tinko.eftimov@uqo.ca

Abstract

In this paper, we propose a lightweight authentication and identification protocol based on different phosphorescent Strontium aluminate color labels. The excitation sources are pulsed UV LEDs emitting at 365 nm and 385 nm, causing different RGB-dependent time responses of the label that are measured using a smartphone recording at 30 FPS. The rise and decay time responses as measured by the red (R), green (G) and blue (B) pixels were separately analyzed and were found to follow a power law with individual parameters depending on the excitation wavelength, pulse duration and duty cycle, which serve as security features and are suitable for authentication purposes in IoT applications. Our solution uses simple cryptographic functions such as HMAC and XOR. We performed a security analysis of our protocol to prove its resistance to known attack vectors. The proposed scheme has minimal computation and communication costs and can be deployed on resource-constrained Internet of Things devices.

Keywords: luminescent security taggants; RGB smartphone detection; IoT security; authentication; cryptographic functions

1. Introduction

The Internet of Things (IoT) is enabling different industries to deploy authentication and identification solutions on resource-constrained devices. Different types of authentication labels are used by industries as a vital component of their anti-counterfeiting systems [1]. It is therefore important that these labels, which are widely deployed in Radio Frequency Identification (RFID) systems [2–4], feature unique or special characteristics that can be leveraged to prevent frauds and counterfeits.

Authentication protocols designed for security labels, e.g., RFID tags [5], must be lightweight due to the minimal resources and capacity of the devices [6]. They must also be resistant to known attacks [3]. A lot of studies have been conducted to propose authentication schemes based on RFID tags [7–11]. However, some of these protocols have been found to have flaws. In their study, Aghili et al. [12] discovered that the lightweight mutual RFID authentication scheme proposed by Fan et al. [7] was not robust against impersonation attacks. Gope et al. [8] designed another lightweight authentication protocol



Received: 17 May 2026

Revised: 27 June 2026

Accepted: 1 July 2026

Published: 7 July 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

that preserves anonymity. However, it was later found to be vulnerable to denial-of-service attacks [10,13]. These limitations underscore the need for more research on authentication protocols and develop new types of labels, e.g., luminescent labels [14].

In their study, Yang et al. [15] proposed a multi-color micro-texture-based physical unclonable function (PUF) fluorescence glass labels (MTPLs). It combines rare-earth ions (RE^{3+}) with bionic micro-texture replication onto transparent glass. A 3D fluorescence QR-Code was proposed by You et al. [16]. To increase the performance of anti-counterfeiting tags in terms of information encryption and storage, Lou et al. [17] proposed a double-lock label based on thermosensitive polymer hydrogels for information camouflage and multi-level encryption. Studies on emerging luminescent materials such as aggregates and room-temperature phosphorescent materials have also been carried out for anti-counterfeiting applications [18]. In order to create new luminescent labels that can be adequately challenged by smartphones, Vitola et al. [19,20] have characterized Eu^{2+} and Dy^{3+} co-doped strontium aluminates with different precursors (Hexamethylenetetramine—HTMA, LiOH , KOH , NaOH , K_2CO_3 , Na_2CO_3 , $(\text{NH}_4)_2\text{CO}_3$). The unique properties of these luminescent labels can be applied to IoT authentication applications.

In this work, we propose a new authentication protocol based on luminescence time response labels. The protocol is lightweight and can resist man-in-the-middle attacks and replay attacks. A simple approach for phosphorescent security labels whose time responses are excitation wavelength-dependent is also proposed.

The rest of the paper is organized as follows. In Section 2, we present the design of the smartphone readable time response luminescent label. In Section 3, we present the authentication method, and we present the conclusion in Section 4. The details of the authentication protocol are presented in Appendix A.

2. Phosphorescent Materials and Smartphone-Readable RGB Color-Dependent Time Responses

2.1. Short-Lifetime Strontium Aluminate Materials

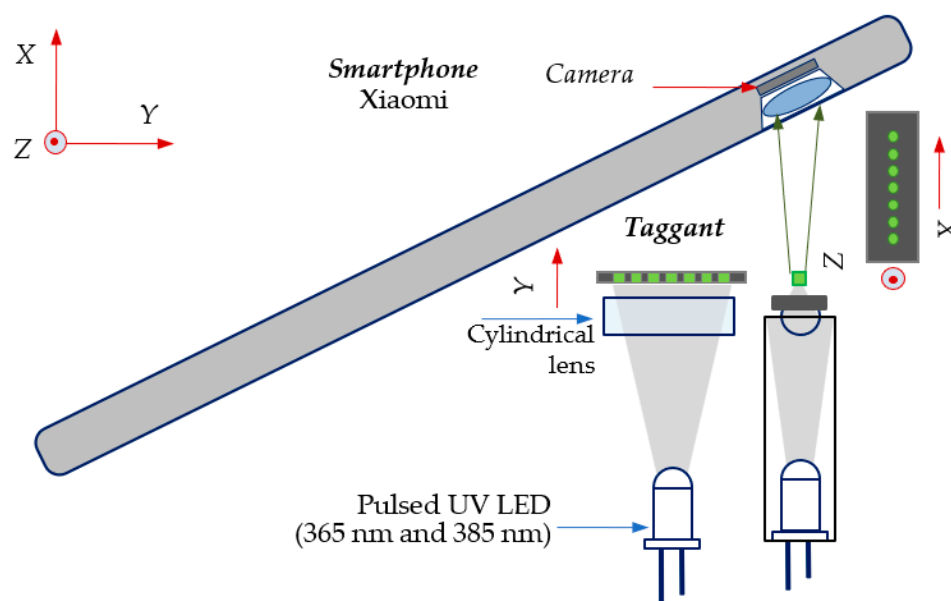
For the purpose of developing affordable photonic security labels for Internet of Things applications, it is desirable to develop photonic readers that are available for the broad public. The best candidate for an interrogation device is the smartphone or lower-cost optoelectronic devices using similar 2D color cameras. These cameras offer the possibility to detect and record videos of the periodically excited luminophors and accurately reproduce their specific rise and decay time responses. As the cameras typically operate at a frame rate of 30 FPS and, more rarely, of 60 FPS, this translates to an inter-frame duration of 33.3 ms and 16.7 ms. To perform a meaningful fit to a rise/decay time response, at least a dozen points would be needed. For a 50% duty factor, this implies that the rise/decay times should be of the order of a second. Thus, among the various long afterglow Strontium aluminates, those of rise/decay times of the order of seconds would be the best fit. Fluorescent materials with nano- and microsecond time responses are inapplicable in this case.

In previous works [19,20], we have proposed and characterized Eu^{2+} and Dy^{3+} co-doped strontium aluminates whose spectral and time responses have been tailored by using different precursors (Hexamethylenetetramine—HTMA, LiOH , KOH , NaOH , K_2CO_3 , Na_2CO_3 , $(\text{NH}_4)_2\text{CO}_3$) in a way that they are within the one-second time response range for use in smartphone detectable optical taggants. Table 1 summarizes the basic differences of the precursors of the samples, the main crystal phase and the trap depths. We have shown that both the spectral and time responses of such materials can be adequately interrogated using smartphones. Their advantage is that their individual time responses, which are detected and registered by the red (R), blue (B), and green (G) pixels, occupy different, though sometimes partially overlapping, spectral ranges.

Table 1. Summary of the seven precursor-tailored Sr aluminate phosphors used for labels in this work (for details, see [21]).

ID	Precursor (Anion)	Main Crystal Phase(s)	Particle Morphology	Trap Depth (eV)
#1	HMTA	Mostly $\text{Sr}_3\text{Al}_2\text{O}_6$ + trace $\text{Sr}_4\text{Al}_{14}\text{O}_{25}$	Compact spheres	0.05/0.17
#2	LiOH	~60% monoclinic SrAl_2O_4 + cubic $\text{Sr}_3\text{Al}_2\text{O}_6$	Fused platelets	0.103
#3	KOH	Monoclinic SrAl_2O_4 rich	Ragged plates	0.055
#4	NaOH	Monoclinic SrAl_2O_4 with $\approx 18\%$ cubic phase	Plate-like	0.161/0.112
#5	K_2CO_3	>90% cubic $\text{Sr}_3\text{Al}_2\text{O}_6$	Smooth quasi spheres	0.117/0.186
#6	Na_2CO_3	Nearly pure $\text{Sr}_3\text{Al}_2\text{O}_6$	Dense spheres	0.148
#7	$(\text{NH}_4)_2\text{CO}_3$	~1:1 monoclinic SrAl_2O_4 /cubic $\text{Sr}_3\text{Al}_2\text{O}_6$ mix	Compact, partly sintered	0.150

Powders from the samples listed in Table 1 were placed in 1 mm diameter holes spaced in a line at 1 mm from one another in a black, non-transparent plate. The arrangement of the taggant containing the seven labels is presented from different views along the X, Y and Z axes as shown in Figure 1.

**Figure 1.** Experimental setup involving a smartphone, with UV LEDs in combination with a glass rod acting as a cylindrical lens illuminating the platform containing the row of the seven phosphorescent labels. In the inset, the X, Y and Z views of the taggant and the LED excitation arrangement are presented.

Two UV LEDs emitting at 365 nm and 385 nm, pulsed at a repetition frequency of $f = 0.5$ s (i.e., a period of $T = 2$ s) and variable duty cycle $\eta = 10\%$, 30% , 50% , 70% and 90% , were used during the experiments. Video clips lasting at least 20 s were taken and the values of every 10 measurements were averaged. The video clips were analyzed using a Python 3.11 script that reads separately the signals from the blue (B), green (G) and red (R) pixels, which are formed from the weighted gray (Y) response.

2.2. RGB Color-Dependent Smartphone Readable Time Responses

The time responses in the spectral ranges covered by the B (blue), G (green), and R (red) pixel transmission filters have been found to be quite different and characteristic for every sample. Firstly, the color of the samples appear different depending on the excitation wavelength (365 nm or 385 nm) as is shown in Figure 2.

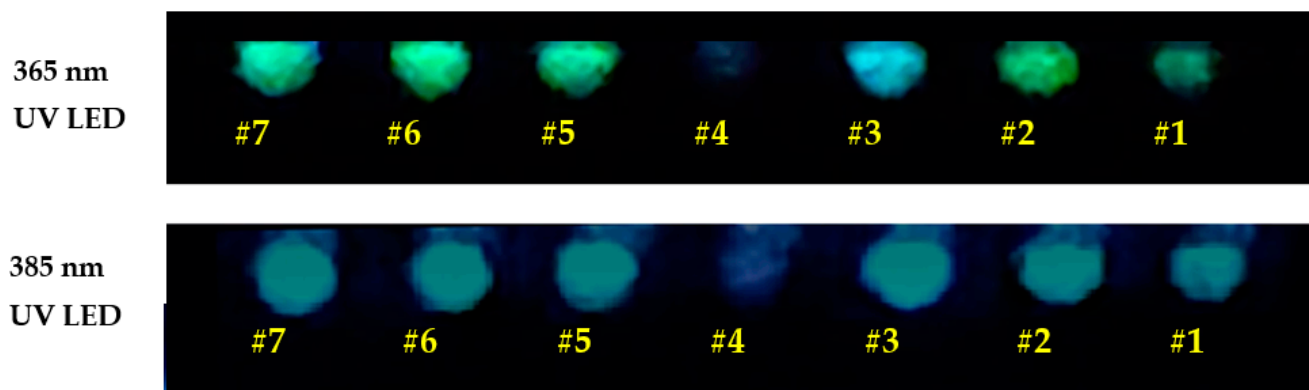


Figure 2. Photos of the luminescent samples from #1 to #7 under 365 and 385 nm UV LED excitation.

It has been found that, for some samples, the time responses in the red spectral range (R) exhibit an anomalous behavior consisting of a non-monotonous decrease in the phosphorescence. The responses in the red spectral range are the weakest of all, since most of the emissions are in blue-green. The blue component appears stronger with 385 nm excitation, possibly because of partial detection of the higher-wavelength wings of the spectral distribution of the excitation 385 nm.

Figure 3a–d show the rise and decay time responses as detected by the blue (B), green (G), and red (R) pixels as well as the weighted (Y) response of samples #1 and #2 under 365 nm UV LED excitation (left column (a) and (c)). The observable differences are characteristic for the rest of the samples. Firstly, it is clearly seen that R, G and B responses essentially differ from one another. The anomalous response in the red is clearly seen for 365 nm excitation (Figure 3a,c). Second, there is an evident difference between the responses with 365 nm and with 385 nm excitation. More specifically, with 365 nm excitation the G-component dominates, while with 385 nm excitation the B-components are stronger. Notably, the rise response in the first case is slower than in the second.

Apart from the excitation wavelength, the particular time responses depend on the duty factor of the excitation pulses, the example of which is shown in Figure 4a–c. As the duty cycle increases, there is more time for electron traps to get populated during the excitation, which increases the luminescence intensities during both excitation and decay as is evidenced in the compound plot from Figure 4d. The above examples show that the rise and decay time responses of every strontium aluminate sample will be different, depending on the excitation wavelength, the color dependence of the time responses, the parameters of the excitation pulses (period and duty cycle), as well as the intensity of the excitation light. Thus, depending on the *challenge* (excitation wavelength, period, duty cycle, temperature and intensity), a particular phosphor will have different *responses*, which makes the response conditional. An authentication protocol can therefore be developed, in which case, values from the time responses corresponding to a randomly chosen challenge will be exchanged between the participants.

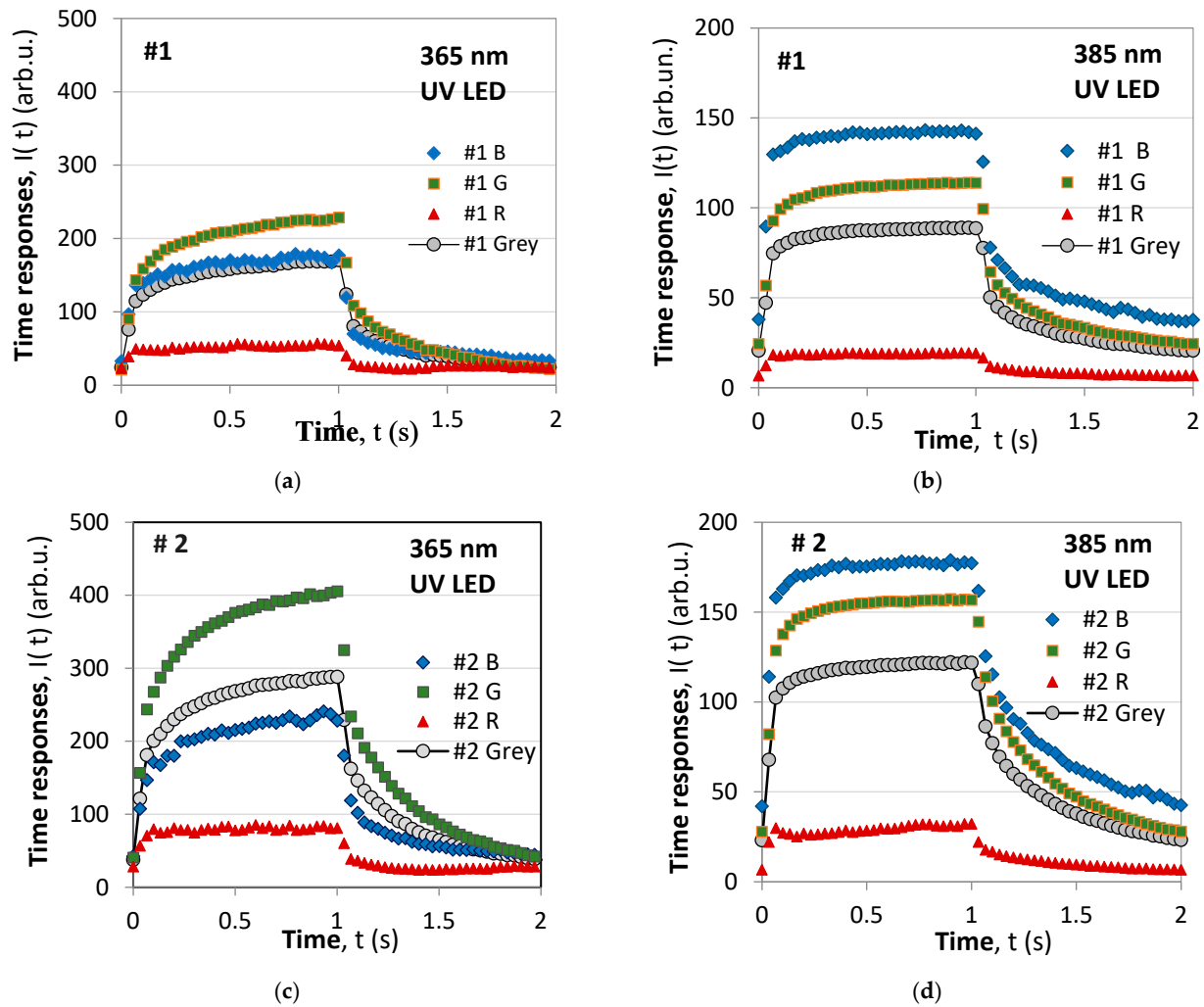


Figure 3. Rise and decay time responses as recovered from the blue (B), green (G), and red (R) pixels along with the corresponding gray response of samples #1 and #2 for 365 nm UV LED excitation (left columns (a,c)) and for 385 nm UV LED excitation (right column (b,d)).

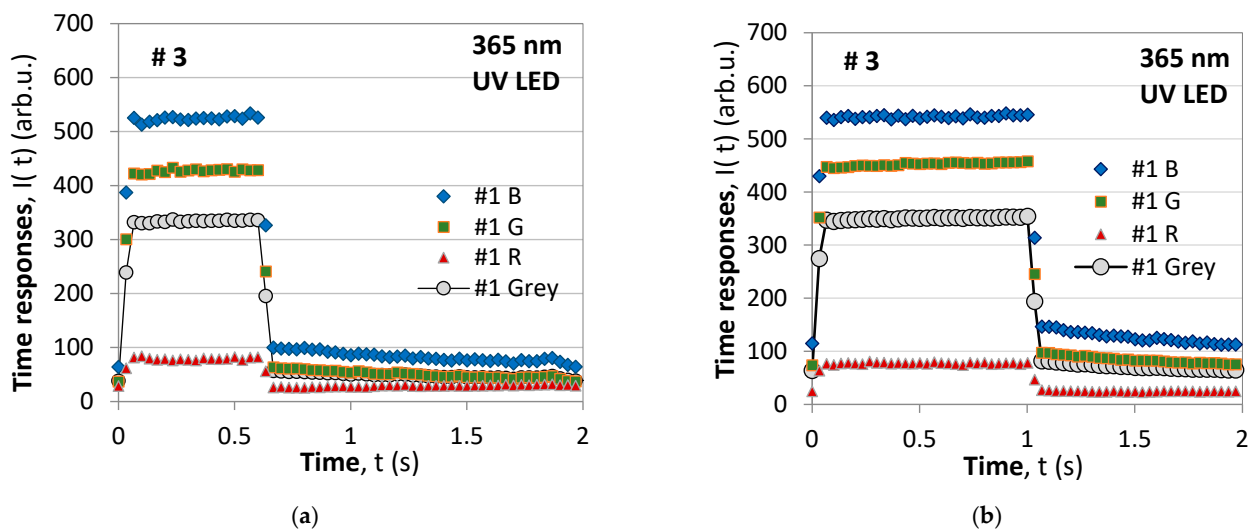


Figure 4. Cont.

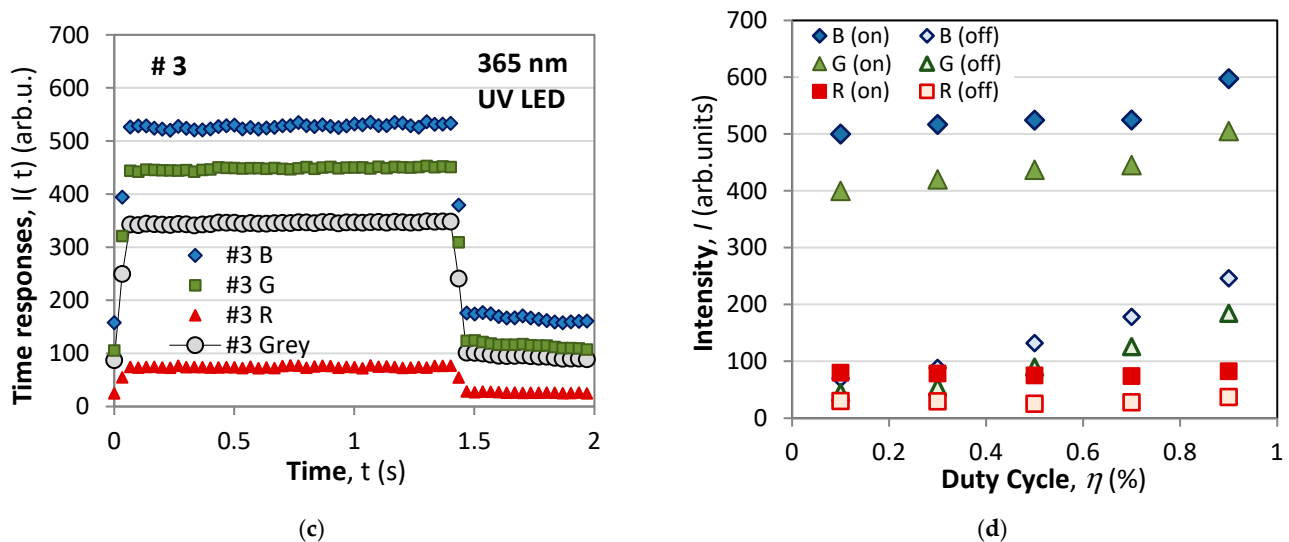


Figure 4. Rise and decay time responses as recovered from the blue (B), green (G), and red (R) pixels and the corresponding gray response of sample #3 for 365 nm UV LED excitation, as well as duty cycles at (a) 30%, (b) 50%, (c) and 70%. (d) A comparison of the average intensities during the ON and the OFF phases for all five duty cycles.

3. Authentication Method and Protocol

3.1. Authentication Method

The authentication process may in principle use different characteristics of the luminescent tag (or taggant) such as color, spectral content, and time response. Here, we consider the specific time responses [20] that are RGB color-dependent, as shown above.

The RGB time responses of a particular arrangement of luminescent taggants that form a label are obtained from a series of ON/OFF pulsed UV LED, the rise/decay time responses of which are taken using a smartphone at a standard 30 FPS frame rate. For a repetition frequency of $f = 0.5$ Hz and a duty cycle $\eta = 50\%$, the ON and OFF durations are 1 s each, which translates into a 30 measurements per rise and decay response. The signals from the R, G, and B pixels are individually analyzed and a resultant weighted Y signal corresponding to a gray color is formed as:

$$Y = A_B B + A_G G + A_R R \quad (1)$$

where B, G, and R are the values from the signals of the blue, green and red pixels, while A_B , A_G , and A_R are the corresponding weight coefficients. Usually, the values $A_B = 0.0721$, $A_G = 0.7154$, and $A_R = 0.2125$ are used so that the gray signal best reflects the particular spectral sensitivities of the human vision. However, these values may seriously deform the shape of the individual spectrum. Thus, other values of the coefficients may be used to more correctly reproduce the observed spectra. In addition, the RGB pixel transmission spectra $T_R(\lambda)$, $T_G(\lambda)$, and $T_B(\lambda)$ partially overlap.

The fundamental problem to solve is how to reduce the number of bits exchanged during the authentication process, but transmit enough information about the time responses, for example, transmit less than 30 values per second per color filter.

3.1.1. Normalized Piece-Wise Power-Law and Exponential Response

The approach we propose in this paper is to transmit the fitting parameters of a given response instead of the individual values. Previous studies [21,22] have shown

that the rise/decay time responses can be approximated sufficiently well with normalized power-law or exponential functions, represented as follows:

$$R_i(t) = \frac{I_{ON,i}(t)}{I_{ON,i,sat}} = 1 - A_0 t^{-\alpha_0} = 1 - \left(\frac{t}{t_R}\right)^{-\alpha_0}, \text{ with } t_R = A_0^{\frac{1}{\alpha_0}} \quad (2)$$

$$D(t) = \frac{I_{OFF,i}(t)}{I_{ON,i,sat}} = A t^{-\alpha} = \left(\frac{t}{t_D}\right)^{-\alpha}, \text{ with } t_D = A^{\frac{1}{\alpha}} (i = B, G, Y) \quad (3)$$

for the power-law responses or

$$R_i(t) = \frac{I_{ON,i}(t)}{I_{ON,i,sat}} = 1 - B_0 e^{-\beta_0 t} = 1 - B_0 e^{-\frac{t}{\tau_0}}, \quad \tau_0 = \frac{1}{\beta_0} \quad (4)$$

$$D(t) = \frac{I_{OFF,i}(t)}{I_{ON,i,sat}} = B t^{-\beta} = B t^{-\frac{t}{\tau}} \quad \tau = \frac{1}{\beta} \quad (i = B, G, Y) \quad (5)$$

for the exponential responses. In Equations (2) and (3), t_R and t_D are the rise and decay time scaling parameters (in seconds) for the power-law responses, while in Equations (4) and (5), τ_0 and τ are the rise and decay constants (in seconds) for the exponential responses.

As previous studies showed [20], the R pixel responses of the strontium aluminates are weaker and, in many cases, exhibit an anomalous time response that cannot be fitted by a power law. We thus chose to use only the time responses of the blue (B), green (G), and gray (Y) pixels. Since the overall response Y is a linear combination (1) of the responses R, G, and B, we can successfully authenticate a label with the characteristic information gained from only three of the four parameters.

An example of the power-law and exponential function of sample #5 is presented in Figure 5 for 385 nm excitation and in Figure 6 for 365 nm. A comparison of the 1-ON and OFF responses and the fitting functions clearly demonstrate that the rise/decay time responses depend on the excitation wavelength. From the graphs of the blue, the green, and the Y-overall time responses, we determine the fitting parameters A_0 , α_0 and A , α . For $T = 2$ s ($f = 0.5$ s) and a duty cycle $\eta = 50\%$ ($\tau_R = \tau_D = 1$ s), the fitting parameters for B, G, and Y are listed in Tables A1–A3 from Appendix A, in which the time parameter t_n represents the number of consecutive video frames ($t_n = 1, 2, 3 \dots$).

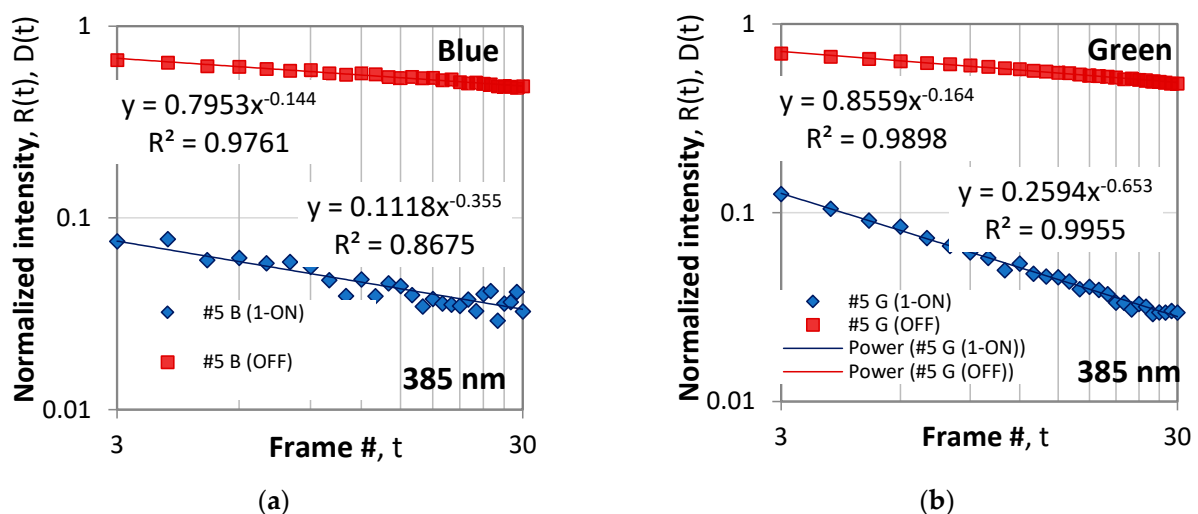


Figure 5. Cont.

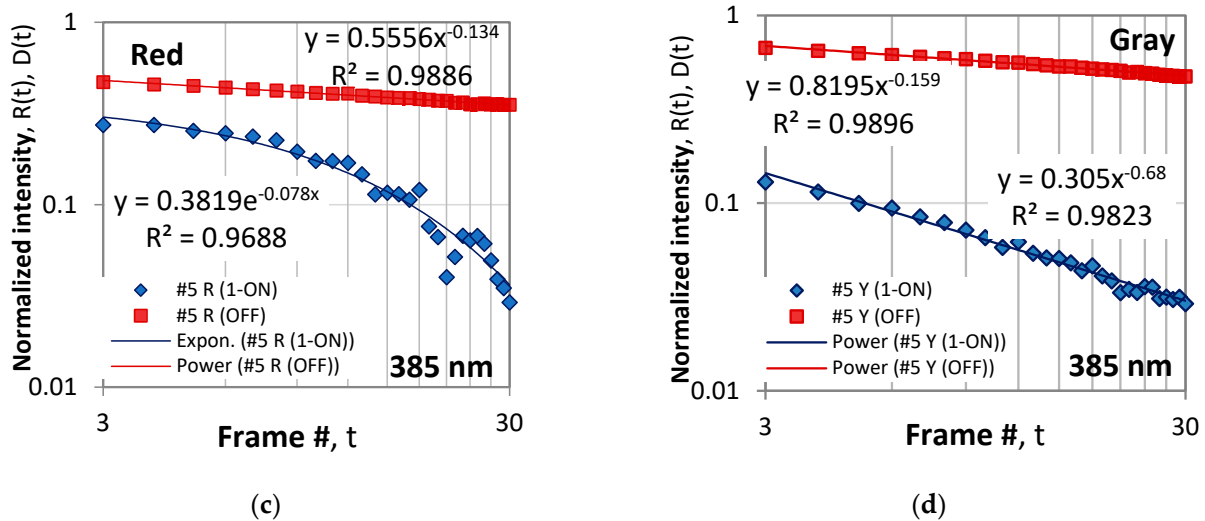


Figure 5. Power-law and exponential fits of 1-ON and OFF time responses of sample #5 for 385 nm excitation for B (a), G (b), R (c) and gray (d) responses. Of all the responses, only the 1-ON response of the red pixels exhibited an exponential response.

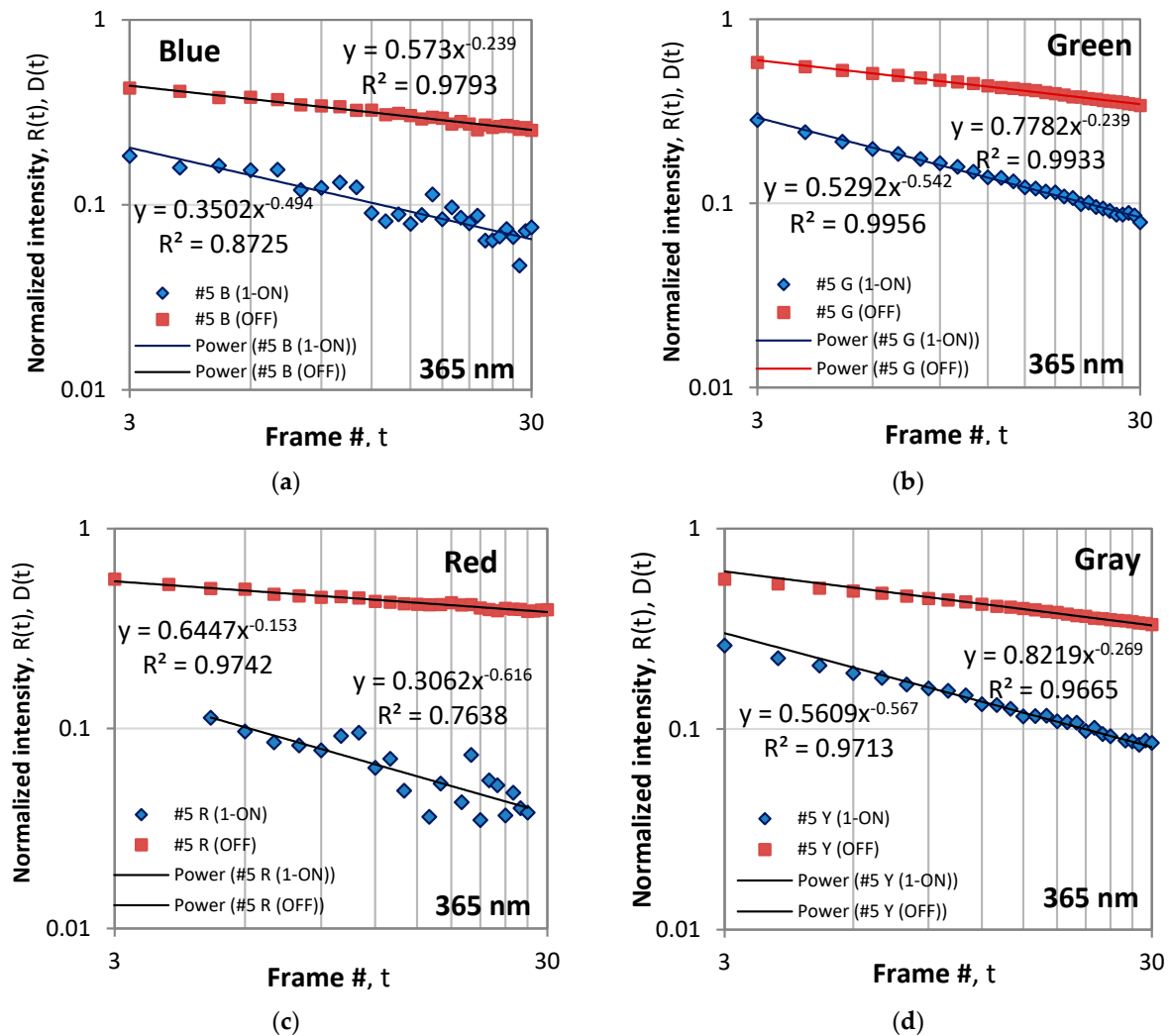


Figure 6. Power-law and exponential fits of the 1-ON and OFF time responses of sample #5 for 365 nm excitation for B (a), G (b), R (c) and gray (d) responses. Of all the responses, only the 1-ON response of the red pixels exhibited an exponential response.

Tables A1–A3 from Appendix A summarize the values of the power-law fitting parameters A_0 , α_0 for the ON phase and A , α for the OFF phase for 385 nm UV LED excitation. For 365 nm excitation, the individual power-law fitting parameters are different. Thus, the RGB time response signatures are conditional on the excitation wavelength. We have also previously shown that they are duty cycle-dependent. Therefore, these findings clearly demonstrate that short lifetime phosphorescent materials are particularly convenient for security taggants.

3.1.2. System Model

The authentication system in our study is composed of a smartphone with a camera and a server where data related to genuine luminescent labels are stored. The two devices can communicate and exchange information related to the luminescent labels. Figure 7 shows the system components and the steps that are performed to authenticate a label. The question then is what format to use so that the individual time responses are identified using a minimum amount of information. Sending the individual values of all 30 or 60 points per second is the most straightforward approach for an ID number, but this approach is sensitive to fluctuations due to noises, especially since the signal is weak at the beginning of the ON and the end of the OFF phases. However, a power-law or an exponential fit reduces the ON and OFF responses to only two numbers per pixel color, for each of the parameters A_0 , α_0 and A , α . Equally simple is to use the related pairs (t_R, α_0) for the ON and (t_D, α) for the OFF phase. To decide which pair is better suited, we imposed an additional condition that the values in the chosen pair are of a comparable order of magnitude.

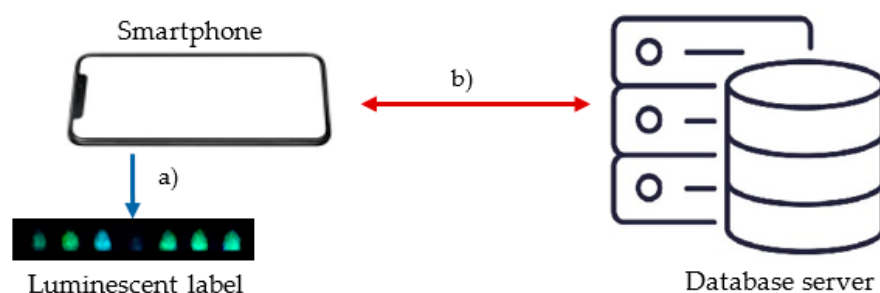


Figure 7. Label authentication system. (a) Step 1: Initialization: The smartphone reads the luminescent, analyzes the time responses, and determines the fitting parameters A_0 , α_0 , A , and α . (b) Step 2: The series of values, as seen in Figure 8 or Figure 9, are then exchanged with the server to authenticate the label.

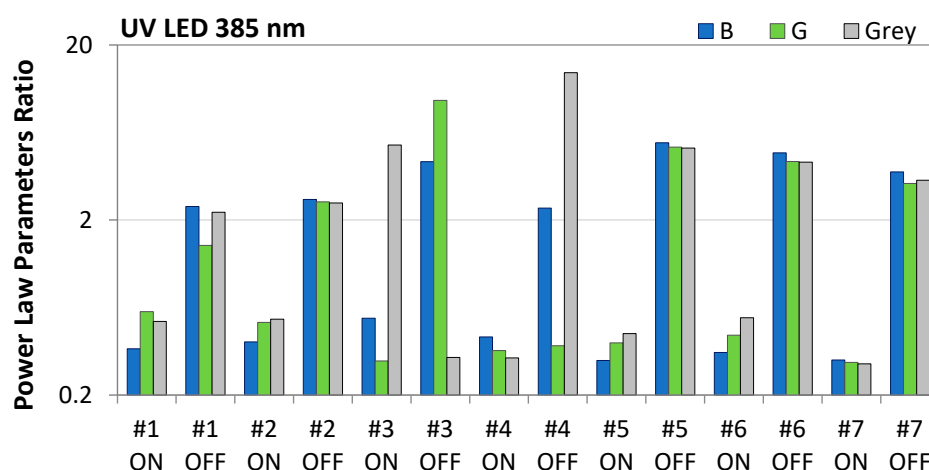


Figure 8. Ratios A_0/α_0 and A/α of the power-law fitting parameters for each of the seven samples.

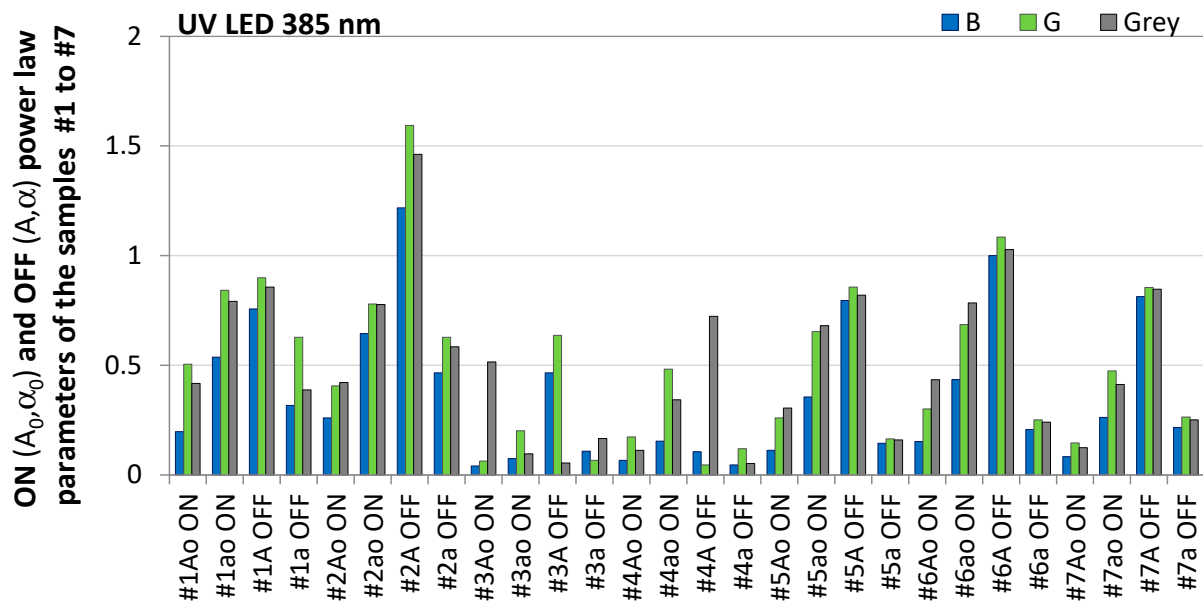


Figure 9. Individual power-law parameters for each sample for the ON and OFF and for each of the three responses B, G, and gray.

Comparing the values from Tables A1–A3, we note that the amplitudes A_0 and A , and the powers α_0 and α vary by less than two orders of magnitude for the ON and the OFF responses. The ratios A_0/α_0 and A/α can serve as a useful measure, from which we have shown for the B, G and gray responses in Figure 7. There, we see that these ratios vary between ≈ 0.3 and ≈ 14 , so the difference is less than 50 times. On the other hand, if we use (1) to calculate the time scaling parameters t_R and t_D , we find that they vary between 1.38 s and 1.89×10^{-22} s, which is unacceptable. We therefore chose the numbers of either the ratios A_0/α_0 and A/α from Figure 8 or of the pairs (A_0, α_0) and (A, α) for each of the B, G and gray responses shown in Figure 9 for identification and authentication purposes. Thus, to identify a sample, choosing the ratios from Figure 8 would require 6 unique ID numbers, versus 12 if the pairs are used. For the above-2 s periodic signals, a 50-level ($L = 50$) quantization of the ID numbers would create binary words of length $\nu = \log_2 L \approx 6$ bits. We would then need 36 bits/s/sample if we use the ratios and 72 bits/s/sample if we choose the pairs. This is a better approach for the resource-constrained IoT devices.

3.1.3. Adversary Model

We consider an adversary TA with the following capabilities:

TA has total control over the communication channel.

TA can intercept, read, and modify messages.

TA can replay previous messages.

TA can learn the hashed value of the temporary identities of the devices.

3.2. Protocol Details

In this section, we present the details of the proposed label authentication protocol with two phases: an initialization phase and a label authentication phase. The notations used in the description are in Table 2.

Table 2. Notations.

Symbols	Definitions
TXDi	Temporary Identity of the devices
$h()$	Hash function
$(.)$	Concatenation
$\oplus$	XOR
hmac	Hash-based Message Authentication Code—HMAC
SIKey	Shared key
ACKGB	Acknowledgment
cmc1, cmc2	HMAC codes
φ_i	Fitting parameters
rand()	Random number generation

3.2.1. Initialization

The first step of the authentication process begins by taking a video of the luminescent labels with a smartphone. The time responses are then processed and the fitting parameters determined see Figure 8 above.

3.2.2. Label Authentication

The label authentication is performed through a series of messages that are exchanged between the smartphone and the server. The smartphone generates a temporary identity $TXD1$ by using a pseudo-random number generator. Two random numbers, ko and pq , are also generated. It then computes $sn0 = (k0, pq)$ and sends a message $msg1 = h(TXD1), sn0$ to the server. The server creates its own temporary identity $TXD2$, generates a random number $k2$, and replies with $msg2 = ((TXD2 \oplus pq), k2)$. After receiving the response from the server, the smartphone sends the fitting parameters $CXT = (sc21, sc22, sc31, sc32, sc41, sc42, sc51)$ to the server. The smartphone also computes a shared key $SIKey = (TXD2 \oplus TXD1)$, creates a HMAC code $cmc1$ using $SIKey$, then sends the message $msg3 = (((TXD1 \oplus pq), (k2 \oplus k1)), sc21, sc22, sc31, sc32, sc41, sc42, sc51, cmc1)$ to the server. Upon receiving $msg3$, the server checks the validity of the parameters and sends an acknowledgment $ACKGB$ to the smartphone. A label is considered genuine when the smartphone verifies that the received acknowledgement is positive. The authentication algorithm is depicted on Figure 10.

3.3. Security Analysis

The results of the security analysis of the protocol are presented in this section.

3.3.1. Informal Security Analysis

We performed an informal security analysis of the protocol and proved its robustness against replay attacks and man-in-the-middle attacks. The proposed protocol can also enforce the data integrity and forward/backward secrecy.

Forward and Backward Secrecy: The proposed protocol achieves forward and backward secrecy. The adversary cannot extract the keys from messages $msg3$ and $msg4$. At the same time, she will be unable to compute the HMAC codes $cmc1$ or $cmc2$. The shared keys of the current session cannot be used in future sessions; additionally, they cannot decrypt previous messages.

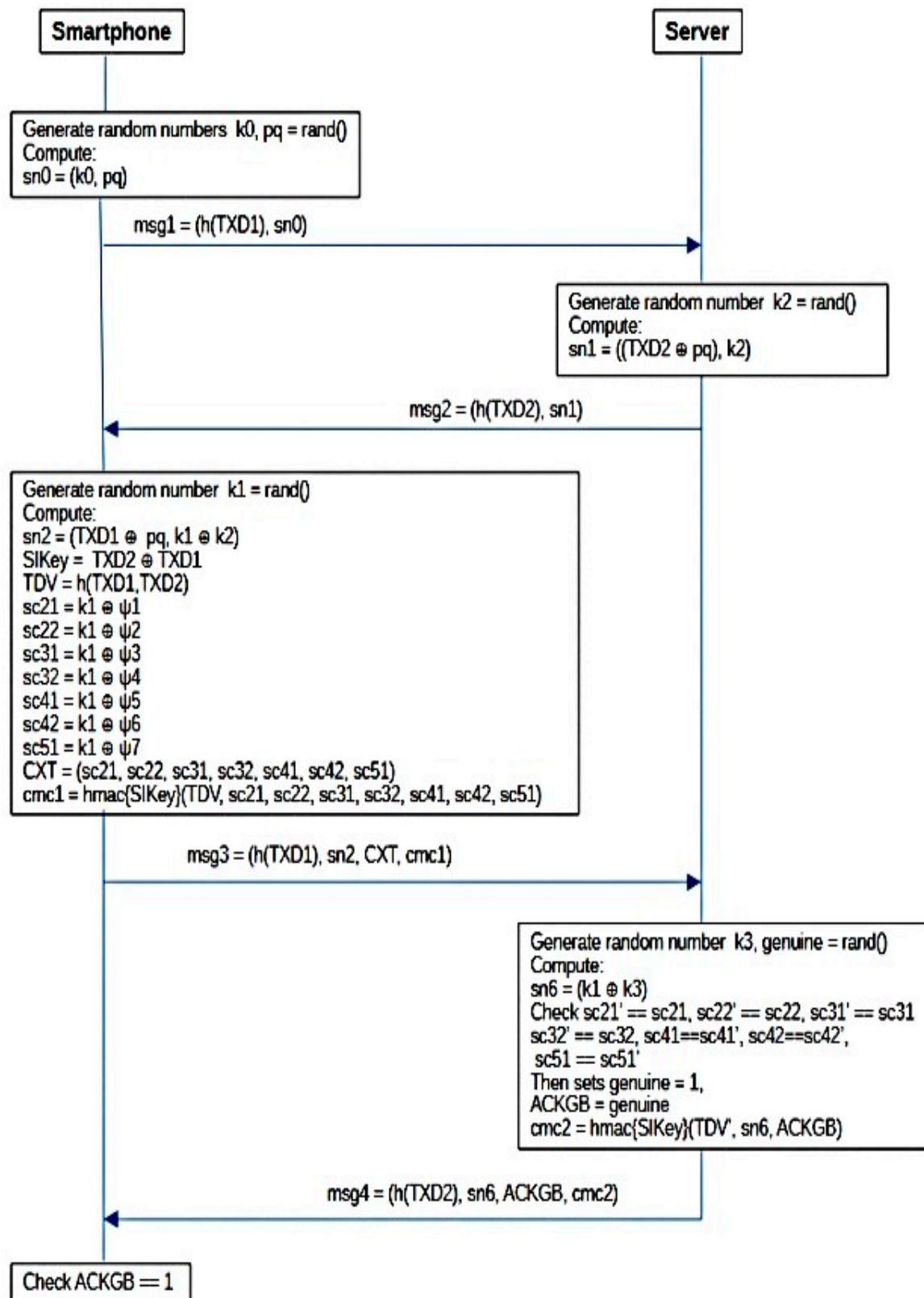


Figure 10. Authentication algorithm.

Man-in-the-Middle Attacks: The adversary cannot successfully conduct a man-in-the-middle attack against the protocol. The adversary cannot guess the value of $sn0$ or $sn1$. Furthermore, she cannot guess the temporary identities of the smartphone and the server. Additionally, she cannot forge the values of $cmc1$ or $cmc2$.

Replay attacks: The proposed protocol is resistant to replay attacks. For example, a replay attack with *msg1* will not succeed because of the temporary identities and the random numbers that are used in *sn0* and *sn1*. Since the adversary cannot guess the shared key *SIKey*, a replay of *msg3* and *msg4* will fail.

Data Integrity: The protocol guarantees the integrity of the data and the messages. The adversary cannot forge the value of *sn0* or the temporary identities of the smartphone and the server. An attempt to forge *msg3* or *msg4* will fail because the adversary cannot forge *SIKey* or the HMAC codes *cmc1* and *cmc2*.

Confidentiality: The data exchanged between the smartphone and the server are protected. The actual identities of the two parties *TXD1* and *TXD2* are protected with a one-way hash function. The relative shares of the RGB colors are also protected in *msg3*.

3.3.2. Security Analysis with Scyther

The security properties of our scheme have been tested with the Scyther tool [23]. The version used for our study is v1.1.3. The software uses claim events, created using the integrated SPDL (Security Protocol Definition Language) scripting language, to verify the security properties of protocols. For example, the claim Secret proves that a given value is confidential. The results of the analysis of our protocol are shown in Table 3. These results prove that, after several rounds of tests, Scyther did not find any potential attack on the protocol.

Table 3. Scyther results.

Claims				Status	Comments
L_AUTH	DV1	L_AUTH_T6	Commit DV2, Concat(XO	OK	No attack within bounds
		L_AUTH_T1	Alive	OK	No attack within bounds
		L_AUTH_T2	Niagree	OK	No attack within bounds
		L_AUTH_T3	Nisynch	OK	No attack within bounds
		L_AUTH_T86	Secret h(XOR(TD1,TD2))	OK	No attack within bounds
	DV2	L_AUTH_B21	Commit DV1, (XOR(n0,	OK	No attack within bounds
		L_AUTH_B23	Alive	OK	No attack within bounds
		L_AUTH_B24	Niagree	OK	No attack within bounds
		L_AUTH_B25	Nisynch	OK	No attack within bounds
		L_AUTH_T59	Secret h(XOR(TD1,TD2))	OK	No attack within bounds
Done					

3.3.3. Formal Security Analysis

The formal proof of the proposed protocol has been performed with BAN logic [24]. The rules and notations are in Appendix B.

Protocol Idealization: The protocol is first idealized as follows, where *S* and *P*, respectively, represent the server and the smartphone:

msg2: $S \rightarrow P: ((TXD2 \oplus pq), k2)$

msg3: $P \rightarrow S: ((TXD1 \oplus pq), (k1 \oplus k2), \langle CXT \rangle_{cmc1})$

msg4: $S \rightarrow P: ((k3 \oplus k1), \langle ACKGB \rangle_{cmc2})$

Idealized Protocol

msg2: $S \rightarrow P: \{ \{Z, P \leftrightarrow Y \rightarrow S\}, H \}, \text{from } S$

msg3: $P \rightarrow S: \{ \{B, U, P \leftrightarrow Y \rightarrow S\}, CXT, cmc1 \}, \text{from } P$

msg4: $S \rightarrow P: \{ \{F, P \leftrightarrow Y \rightarrow S\}, ACKGB, cmc2 \}, \text{from } S$

Goals: We identify the following goals for our protocol.

G1: The smartphone believes the temporary identity (TXD2) of the server is fresh.

G2: The server believes the temporary identity (TXD1) of the smartphone is fresh.

G3: The smartphone believes the acknowledgment sent by the server.

Assumptions:

A1: $P \models S \leftrightarrow Y \rightarrow P$

A3: $P \models \#(pq)$

A7: $P \models S \Rightarrow TXD2$

A9: $P \models \sim(pq)$

A10: $S \models P \leftrightarrow Y \rightarrow S$

A22: $S \models \#(pq)$

A50: $S \models P \Rightarrow TDX1$

A33: $P \models \#(k1)$

A35: $P \models \sim k1$

A55: $S \models \sim(k3)$

A61: $P \models S \Rightarrow k3$

Proof

Step 1: $P \triangleleft ((Z), H)$

Step 2: $P \triangleleft (Z)$

Step 3: $P \models S \models \sim(TXD2, pq)$

Step 4: $P \models S \models (TXD2, pq)$

Step 5: $P \models S \models (TXD2)$

Step 6: $P \models TXD2$

Step 7: $P \models \#(TXD2, pq)$

Step 8: $S \triangleleft (B, U, CXT, cmc1)$

Step 9: $S \triangleleft B$

Step 10: $S \models P \models \sim(TXD1, pq)$

Step 11: $S \models P \models (TDX1, pq)$

Step 12: $S \models (TDX1, pq)$

Step 13: $S \models \#(TDX1, pq)$

Step 14: $P \triangleleft (F, ACKGB, cmc2)$

Step 15: $P \triangleleft F$

Step 16: $P \models S \models \sim(k3, k1)$

Step 17: $P \models S \models (k3, k1)$

Step 18: $P \models S \models (k3)$

Step 19: $P \models (k3)$

Step 20: $P \models (k3, k1)$

Step 21: $P \models ((k3, k1), ACKGB)$

R4-A

A1, R1

A3, A9, R2

R6-C

A7, R3

A3, A9, R5-A

C1—Goal 1

R4-A

A10, R1

A22, R2

A50 and R3

A22, R5-A

C2—Goal 2

R4-A

A1, R1

A33, A35, A55, R2

R6-C

A61, R3

R5-A

R5-A

Goal—3

3.4. Performance Evaluation

We evaluated the performance of our protocol by comparing its communication and computation costs to relevant solutions: Cho et al. [25], Gope et al. [8], and Mansoor et al. [13]. The implementation platform was composed of an Android Studio Koala 2024 [26] with the cryptographic library CRYPTO++ version 8.6.0 [27], installed on an HP machine running Windows 11 operating system on an AMD Ryzen 3x5300U processor and 8 Gb RAM.

3.4.1. Computation Cost

The time required to compute one hash and one HMAC code are, respectively, represented by T_h and T_{hmac} . The XOR and the concatenations have extremely low cost and are not included in the total computation cost of the protocol. The execution time for one T_h is 0.006 ms and the execution time for one T_{hmac} is 0.0075 ms. Table 4 summarizes the computation costs of the protocols. The total computation cost of our protocol is $5T_h + 2T_{hmac}$. Assuming the almost-equal cost of T_h and T_{hmac} , and by considering only the cost between the reader and the server in the schemes in [8,25] and [13], we can observe that the total computation cost of our protocol is less than [8]; it is equal to the scheme in [25]. The cost is, however, greater than the scheme in [13].

Table 4. Summary of the computation costs.

	[25]	[8]	[13]	[Our Work]
T_h	7	9	6	5
T_{hmac}	0	0	0	2

3.4.2. Communication Cost

The communication cost of our protocol is also evaluated against the other protocols [8,13,25].

The random number pq , the temporary identities, and the symmetric keys are 8 bytes long, while all the other random numbers are 5 bytes long. We used SHA-1 to compute the HMAC codes. The total communication cost of our protocol is 1565 bits. We summarize in Table 5 the communication cost of the proposed protocol compared to the three relevant ones. We only consider the communication cost between the reader and the server for the three other schemes. According to the table, the total communication cost of our protocol is higher than the schemes of Cho et al. [25] and Mansoor et al. [13]. However, it is only slightly higher than the scheme in [8].

Table 5. Summary of the communication costs.

	[25]	[8]	[13]	[Our Work]
Cost	768	1468	1152	1565

4. Conclusions

In this study, a new luminescent label has been developed as an alternative to the RFID taggants. The label is readable by smartphones and can generate different energy levels under UV light excitation. The excitation sources are UV LEDs emitting at 365 nm and 385 nm, causing different RGB-dependent time responses of the labels. These time responses are then used to authenticate the labels. The main findings of our work are: (1) the time responses are conditional on the excitation wavelength; (2) they are also duty cycle-dependent. These findings demonstrate that short-lifetime phosphorescent materials are particularly convenient for security taggants. The authentication protocol can resist man-in-the-middle attacks and replay attacks. Additionally, the proposed scheme guarantees data integrity and forward/backward secrecy. A comparison with relevant RFID schemes proves that our scheme can be deployed in IoT environments.

Author Contributions: Conceptualization, T.E.; Methodology, Y.A. and V.V.; Software, Y.A., K.N. and A.S.; Validation, K.N. and K.K.; Formal analysis, T.E. and Y.A.; Investigation, V.V. and K.K.; Resources, V.V.; Data curation, K.N.; Writing—original draft, Y.A. and T.E.; Funding acquisition, T.E. and V.V. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by NSERC (Natural Sciences and Engineering Research Council of Canada) Canada through a Discovery Grant DDG-2025-00037. Financial support provided by Fundamental and applied Research project Nr.LZP-2023/1–0521 and realized at the Institute of Solid-State Physics, University of Latvia, is greatly acknowledged.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors on request.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A

In the tables below, we list the power-law parameters for $T = 2$ s ($f = 0.5$ s) and a duty cycle $\eta = 50\%$ ($\tau_R = \tau_D = 1$ s) for a 385 nm LED excitation.

Table A1. Rise and decay power-law fitting parameters for the blue (B) responses (385 nm UV LED).

#	1-ON (B) Blue	R ²	OFF (B) Blue	R ²
#1	$1-0.1973t^{-0.537}$	R ² = 0.8946	$0.7567(t-30)^{-0.317}$	R ² = 0.9836
#2	$1-0.2594t^{-0.644}$	R ² = 0.943	$1.2176(t-30)^{-0.465}$	R ² = 0.988
#3	$1-0.0407t^{-0.074}$	R ² = 0.4434	$0.6366(t-30)^{-0.064}$	R ² = 0.9438
#4	$1-0.0661t^{-0.154}$	R ² = 0.2496	$0.1053(t-30)^{-0.045}$	R ² = 0.6163
#5	$1-0.1118t^{-0.355}$	R ² = 0.811	$0.7953(t-30)^{-0.144}$	R ² = 0.9746
#6	$1-0.1522t^{-0.435}$	R ² = 0.8725	$1.0003(t-30)^{-0.207}$	R ² = 0.9851
#7	$1-0.0831t^{-0.262}$	R ² = 0.6971	$0.8126(t-30)^{-0.216}$	R ² = 0.9866

Table A2. Rise and decay power-law fitting parameters for the green (G) responses (385 nm UV LED).

#	1-ON (G) Green	R ²	OFF (G) Green	R ²
#1	$1-0.5047t^{-0.842}$	R ² = 0.9945	$0.8985(t-30)^{-0.422}$	R ² = 0.9968
#2	$1-0.4056t^{-0.779}$	R ² = 0.976	$1.5932(t-30)^{-0.627}$	R ² = 0.9842
#3	$1-0.0629t^{-0.201}$	R ² = 0.9072	$0.4656(t-30)^{-0.108}$	R ² = 0.9928
#4	$1-0.1732t^{-0.482}$	R ² = 0.8596	$0.0455(t-30)^{-0.119}$	R ² = 0.8729
#5	$1-0.2594t^{-0.653}$	R ² = 0.9912	$0.8559(t-30)^{-0.164}$	R ² = 0.99
#6	$1-0.3008t^{-0.685}$	R ² = 0.9907	$1.0839(t-30)^{-0.251}$	R ² = 0.9815
#7	$1-0.1456t^{-0.474}$	R ² = 0.9798	$0.8546(t-30)^{-0.264}$	R ² = 0.9952

Table A3. Rise and decay power-law fitting parameters for the gray (Y) responses (385 nm UV LED).

#	1-ON (Y) Gray	R ²	OFF (Y) Gray	R ²
#1	$1-0.4168t^{-0.791}$	R ² = 0.9909	$0.8566(t-30)^{-0.387}$	R ² = 0.9969
#2	$1-0.4214t^{-0.777}$	R ² = 0.9886	$1.4618(t-30)^{-0.584}$	R ² = 0.9862
#3	$1-0.515t^{-0.096}$	R ² = 0.9882	$0.0545(t-30)^{-0.166}$	R ² = 0.8683
#4	$1-0.1116t^{-0.342}$	R ² = 0.7686	$0.0723(t-30)^{-0.052}$	R ² = 0.7256
#5	$1-0.305t^{-0.68}$	R ² = 0.9819	$0.8195(t-30)^{-0.159}$	R ² = 0.9896
#6	$1-0.4338t^{-0.784}$	R ² = 0.9874	$1.0276(t-30)^{-0.24}$	R ² = 0.9841
#7	$1-0.1243t^{-0.412}$	R ² = 0.9614	$0.8469(t-30)^{-0.251}$	R ² = 0.9954

Appendix B

BAN LOGIC

LOGICAL POSTULATES

Message-meaning rule (R1)

$$P \models Q \stackrel{K}{\vdash} P, P \triangleleft \{X\}_K \vdash P \models Q \mid \sim X$$

If P believes that the key K is shared with Q and sees a message X encrypted under K, then P believes that Q once said X.

Nonce Verification rule (R2)

$$P \models \#(X), P \models Q \mid \sim X \vdash P \models Q \models X$$

If P believes that X could have been uttered only recently, and that Q once said X, then P believes that Q believes X.

Jurisdiction rule (R3)

$$P \models Q \Rightarrow X, P \models Q \models X \vdash P \models X$$

If P believes that Q has jurisdiction over X, then P trusts Q on the truth of X.

Formula seeing rule (R4)

$$A- P \triangleleft (X, Y), \vdash P \triangleleft X$$

If P sees the combined formula (X,Y), then P sees X

$$B- P \models Q \stackrel{K}{\vdash} P, P \triangleleft \{X\}_K \vdash P \triangleleft X$$

If P believes that the key K is shared with Q and sees a message X encrypted under K, then P sees X

Freshness rule (R5)

$$A- P \models \#(X) \vdash P \models \#(X, Y)$$

$$B- P \models \#(X) \vdash P \models \#(X)_K$$

If one part of a formula is fresh, then the entire formula is fresh

Belief rule (R6)

$$A- P \models X, P \models Y \vdash P \models (X, Y)$$

$$B- P \models (X, Y), \vdash P \models X$$

$$C- P \models Q \models (X, Y) \vdash P \models Q \models X$$

$$D- P \models Q \mid \sim (X, Y) \vdash P \models Q \mid \sim X$$

P believes a set of statements if and only if P believes each individual statement separately

References

1. Choudhury, S.; Costa, F.; Manara, G.; Genovesi, S. Combating the Counterfeit: A Review on Hardware-Based Anticounterfeiting Technologies. *Appl. Sci.* **2025**, *15*, 10298. [\[CrossRef\]](#)
2. Khalil, G.; Doss, R.; Chowdhury, M. A Comparison Survey Study on RFID Based Anti-Counterfeiting Systems. *J. Sens. Actuator Netw.* **2019**, *8*, 37. [\[CrossRef\]](#)
3. Abdulghani, H.A.; Nijdam, N.A.; Konstantas, D. Analysis on Security and Privacy Guidelines: RFID-Based IoT Applications. *IEEE Access* **2022**, *10*, 131528–131554. [\[CrossRef\]](#)
4. Moras, M.; Martínez-Domingo, C.; Escudé, R.; Herrojo, C.; Paredes, F.; Terés, L.; Martín, F.; Ramon, E. Programmable Organic Chipless RFID Tags Inkjet Printed on Paper Substrates. *Appl. Sci.* **2021**, *11*, 7832. [\[CrossRef\]](#)
5. Baashirah, R.; Abuzneid, A. Survey on Prominent RFID Authentication Protocols for Passive Tags. *Sensors* **2018**, *18*, 3584. [\[CrossRef\]](#) [\[PubMed\]](#)
6. Gao, M.; Lu, Y. URAP: A new ultra-lightweight RFID authentication protocol in passive RFID system. *J. Supercomput.* **2022**, *78*, 10893–10905. [\[CrossRef\]](#)
7. Fan, K.; Zhu, S.; Zhang, K.; Li, H.; Yang, Y. A Lightweight Authentication Scheme for Cloud-based RFID Healthcare Systems. *IEEE Netw.* **2019**, *33*, 44–49. [\[CrossRef\]](#)

8. Gope, P.; Hwang, T. A realistic lightweight authentication protocol preserving strong anonymity for securing RFID system. *Comput. Secur.* **2015**, *55*, 271–280. [\[CrossRef\]](#)
9. Kumar, V.; Kumar, R.; Khan, A.A.; Kumar, V.; Chen, Y.-C.; Chang, C.-C. RAFI: Robust Authentication Framework for IoT-Based RFID Infrastructure. *Sensors* **2022**, *22*, 3110. [\[PubMed\]](#)
10. Liu, B.; Yang, B.; Su, X. An Improved Two-Way Security Authentication Protocol for RFID System. *Information* **2018**, *9*, 86. [\[CrossRef\]](#)
11. Zhu, F.; Li, P.; Xu, H.; Wang, R. A Novel Lightweight Authentication Scheme for RFID-Based Healthcare Systems. *Sensors* **2020**, *20*, 4846. [\[CrossRef\]](#) [\[PubMed\]](#)
12. Aghili, S.F.; Mala, H. Security Analysis of an Ultra-Lightweight RFID Authentication Protocol for M-commerce. *Int. J. Commun. Syst.* **2019**, *32*, e3837.
13. Mansoor, K.; Ghani, A.; Chaudhry, S.A.; Shamshirband, S.; Ghayyur, S.A.K.; Mosavi, A. Securing IoT-based RFID systems: A robust authentication protocol using symmetric cryptography. *Sensors* **2019**, *19*, 4752. [\[PubMed\]](#)
14. Yu, X.; Zhang, H.; Yu, J. Luminescence anti-counterfeiting: From elementary to advanced. *Aggregate* **2021**, *2*, 20–34.
15. Yang, J.; Feng, M.; Wang, J.; Zhao, Z.; Xu, R.; Chen, Z.; Zhang, K.; Khan, A.; Han, Y.; Song, F.; et al. Bionic Micro-Texture Duplication and RE³⁺ Space-Selective Doping of Unclonable Silica Nanocomposites for Multilevel Encryption and Intelligent Authentication. *Adv. Mater.* **2023**, *35*, 2306003.
16. You, M.; Lin, M.; Wang, S.; Wang, X.; Zhang, G.; Hong, Y.; Dong, Y.; Jin, G.; Xu, F. Three-dimensional quick response code based on inkjet printing of upconversion fluorescent nanoparticles for drug anti-counterfeiting. *Nanoscale* **2016**, *8*, 10096–10104. [\[CrossRef\]](#) [\[PubMed\]](#)
17. Lou, D.; Sun, Y.; Li, J.; Zheng, Y.; Zhou, Z.; Yang, J.; Pan, C.; Zheng, Z.; Chen, X.; Liu, W. Double Lock Label Based on Thermosensitive Polymer Hydrogels for Information Camouflage and Multi-level Encryption. *Angew. Chem. Int. Ed.* **2022**, *61*, e202117066. [\[CrossRef\]](#) [\[PubMed\]](#)
18. Li, Y.; Gao, P. Emerging Luminescent Materials for Information Encryption and Anti-Counterfeiting: Stimulus-Response AIEgens and Room-Temperature Phosphorescent Materials. *Chemosensors* **2023**, *11*, 489. [\[CrossRef\]](#)
19. Vitola, V.; Dile, M.; Krizmane, K.; Einbergs, E.; Eftimov, T.; Nikolov, K.; Fouzar, S. Tailoring the luminescence properties of strontium aluminate phosphors for unique smartphone detectable optical tags. *Crystals* **2025**, *15*, 474. [\[CrossRef\]](#)
20. Vitola, V.; Eftimov, T.; Nikolov, K.L.; Fouzar, S.; Krizmane, K. Temperature and emission wavelength dependent time responses of strontium aluminates. *Crystals* **2025**, *15*, 744. [\[CrossRef\]](#)
21. Huntley, D.J. An explanation of the power-law decay of luminescence. *J. Phys. Condens. Matter* **2006**, *18*, 1359–1365. [\[CrossRef\]](#)
22. Eftimov, T.; Kostova, I.; Arapova, A.; Patronov, G. Rise and decay time responses of Sr aluminate phosphorescent materials. *J. Lumin.* **2021**, *235*, 117985. [\[CrossRef\]](#)
23. Cremers, C.J. The Scyther Tool: Verification, Falsification, and Analysis of Security Protocols. In *Proceedings of the 20th International Conference on Computer Aided Verification, Princeton, NJ, USA, 7–14 July 2008*; Springer: Berlin/Heidelberg, Germany, 2008; pp. 414–418.
24. Burrows, M.; Abadi, M.; Needham, R. A logic of authentication. *ACM Trans. Comput. Syst.* **1990**, *8*, 18–36. [\[CrossRef\]](#)
25. Cho, J.S.; Jeong, Y.S.; Park, S.O. Consideration on the brute-force attack cost and retrieval cost: A hash-based radio-frequency identification (RFID) tag mutual authentication protocol. *Comput. Math. Appl.* **2015**, *69*, 58–65.
26. Android Studio; Google. Android Studio and SDK Tools. Available online: <https://developer.android.com/studio> (accessed on 10 September 2024).
27. Weidai11. Cryptopp Releases. Available online: <https://github.com/weidai11/cryptopp/releases> (accessed on 12 November 2024).

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.