



(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
06.12.2017 Bulletin 2017/49

(51) Int Cl.:
G09C 5/00 (2006.01) **H04L 9/08 (2006.01)**
H04L 9/32 (2006.01)

(21) Application number: **16172091.7**

(22) Date of filing: **31.05.2016**

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
 Designated Extension States:
BA ME
 Designated Validation States:
MA MD

- **LETZ, Martin**
55128 Mainz (DE)
- **MOSK, Allard**
7523LE Enschede (NL)
- **PINKSE, Pepijn**
7522KJ Enschede (NL)

(71) Applicants:
 • **Schott AG**
55122 Mainz (DE)
 • **Universiteit Twente**
7522 NB Enschede (NL)

(74) Representative: **Blumbach Zinngrebe Patentanwälte**
Alexandrastrasse 5
65187 Wiesbaden (DE)

(72) Inventors:
 • **DAVIS, Mark J.**
Clarks Summit, PA Pennsylvania 18411 (US)

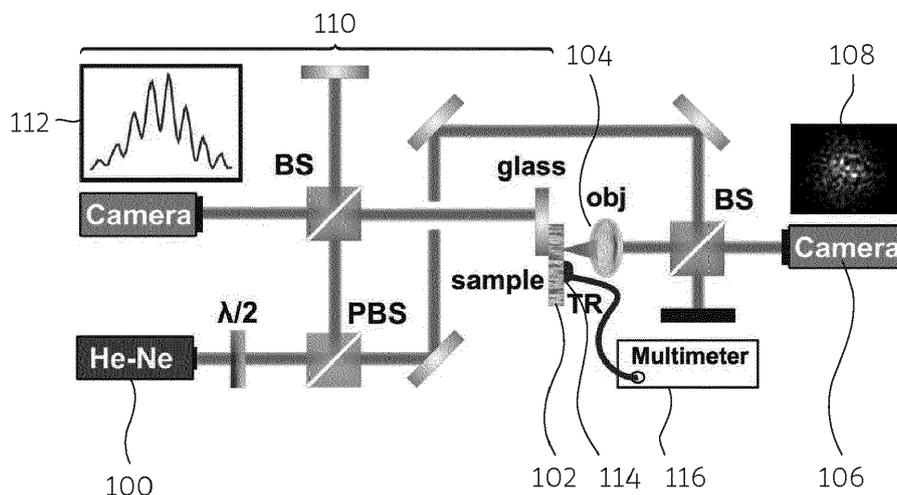
Remarks:
 Amended claims in accordance with Rule 137(2) EPC.

(54) **OPTICAL KEY PROTECTED QUANTUM AUTHENTICATION AND ENCRYPTION**

(57) The invention relates to an apparatus for authenticating an optical key, wherein the optical key is characterized by a reliable authenticatability. The invention also relates to an apparatus for generating a random number from an optical key, wherein the random number is stable

when or after the optical key is exposed to an external influence, in particular a physical or chemical stimulus such as a different ambient condition, mechanical stress or chemical contact.

Fig. 3



Description

[0001] The invention relates to the field of authentication and encryption using optical keys.

[0002] Secure authentication as well as encryption is gaining increasing importance for communication and exchange of confidential information. Authentication and encryption are closely linked technologies, whereat both of which can benefit in terms of security when using physical keys instead of digital keys. A physical key is a physical object characterized by a unique structure, typically of microscopic scale, which originates from random influences during the process of manufacture. Thus, a physical key is practically impossible to replicate. The microscopic random signature of the physical key - or the physical key itself - is often referred to as a physical unclonable function (PUF). Often, the microscopic random signature can be utilized by optical methods, that is, the physical key is an optical (physical) key.

[0003] The EP 2 693 685 A1 provides a quantum secure device, system and method for verifying challenge-response pairs using a physical unclonable function (PUF).

[0004] The US 2013/0243187 A1 discloses a device, including one or more communication physical unclonable function (CPUF) and key storage devices.

[0005] The WO 2007/046018 A1 discloses a device for creating challenge-response pairs with an integrated physical unclonable function (PUF) with combined sensor and display.

[0006] The US 2008/0121708 A1 describes an identity credential or card comprising a substrate conveying information related to an individual, and further comprising a phase-changing medium that serves to vary a directional albedo function.

[0007] Further scientific references in this field are the following:

J. Buchanan, R. Cowburn, A. Jausovec, D. Petit, P. Seem, G. Xiong, D. K. Fenton, D. Allwood, and M. Bryan, Forgery: Fingerprinting documents and packaging, Nature 436, 475 (2005).

S. A. Goorden, M. Horstmann, A. P. Mosk, B. Škorić and P. W. H. Pinkse, Quantum-secure authentication of a physical unclonable function Optica 1, 421 (2014).

A.P. Mosk A. Lagendijk, G. Lerosey, and M. Fink, Controlling waves in space and time for imaging and focusing in complex media, Nat. Photon. 6, 283 (2012).

R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, Physical One-Way Functions, Science 297, 2026 (2002).

R. Horstmeyer, B. Judkewitz, I. M. Vellekoop, S. Assaworrorarit, and C Yang, Physical key-protected one-time pad, Sci. Rep. 3, 3543 (2013).

[0008] A typical setup for the authentication of an optical key comprises a light source for irradiating the optical key in order to exploit its unique signature. The same applies for common setups for the generation of random numbers from an optical key, which can be used for encryption. Since the PUF of the optical key is usually exploited by illumination, suitable materials for producing optical keys are strongly scattering materials. Moreover, strongly scattering objects are suited particularly since the speckle pattern, which is obtained by illuminating the strongly scattering object, contains a combination of coherent and incoherent scattering contributions such that slight microscopic changes in the scattering medium have dramatic consequences for the speckle pattern.

[0009] However, practical applications suffer from the problem that the speckle pattern also depends in a highly sensitive manner on a variety of parameters of the setup comprising the optical key. This dependence on slight changes within the setup, which may even be hard to control, hinders a reliable operation of the devices under non-laboratory conditions and especially in everyday use.

[0010] An object of the invention is to enhance the reliability of setups comprising an optical key and to improve their robustness, particularly for non-laboratory conditions.

[0011] An aspect of the object of the invention is to enhance the practical reliability of the authentication of an optical key, particularly for quantum secure authentication.

[0012] Another aspect of the object of the invention is to enhance the practical reliability of random number generation from an optical key, particularly for encryption or one-time pad encryption.

[0013] The object of the invention is solved by the subject matters of the independent claims. Advantageous embodiments of the invention are subject matters of the dependent claims.

[0014] The invention provides an apparatus for authenticating an optical key by verifying a match of a challenge-response pair.

[0015] The apparatus comprises a challenge forming device for forming a challenge.

[0016] The challenge formed by the challenge forming device may, in particular, be a spatially modulated light wave. That is, the challenge forming device may be designed as a spatial light modulator (SLM) or may comprise a SLM. The

challenge forming device may be adjustable such that the challenge forming device can adopt one of a plurality of settings. For example, the SLM may comprise an adjustable array to impose one of a plurality of spatially varying modulations on the light beam.

5 [0017] The apparatus may further comprise a preferably coherent radiation source to irradiate the challenge forming device. In particular, the apparatus may comprise a radiation source, for emitting radiation comprising quanta. The radiation source may preferably be an electromagnetic radiation source for emitting electromagnetic radiation comprising photons. The radiation may strike on the challenge forming device to introduce for example spatial modulations into the radiation in order to form a (radiation) challenge. In other words, the challenge forming device may be irradiatable by the radiation source and the challenge forming device may in particular be adapted for forming the challenge when being irradiated by radiation emitted by the radiation source.

10 [0018] Further, the apparatus comprises an optical key, which is receptive to the challenge formed by the challenge forming device, for providing a response to the challenge when receiving the challenge formed by the challenge forming device. The optical key comprises a scattering material, in particular a strongly scattering medium. The scattering material may be an inorganic scattering material. In other words, the optical key may provide a nano- or microstructure which determines the response of the optical key to a challenge. The nano- or microstructure preferably is arranged in a volumetric manner (3D), although it shall not be excluded that the structure may be arranged in a planar manner, for example on a surface (2D). The optical key and/or the nano- or microstructure may be denoted as physical unclonable function (PUF).

15 [0019] Further, the apparatus comprises a response verifying device, which is receptive to the response provided by the optical key, for verifying if the response provided by the optical key matches the challenge formed by the challenge forming device.

20 [0020] The response verifying device may, for example, comprise a SLM. The response verifying device may in particular be adjustable in a similar way as the challenge forming device, whereat each setting of the response verifying device may match one setting of the challenge forming device. In other words, the response verifying device may adapt one specific of a plurality of settings. The specifically selected setting of the response verifying device may preferably be related to the selected setting of the challenge forming device. In other words, each setting of the plurality of settings of challenge forming device may be related to exactly one setting of the plurality of settings of challenge forming device.

25 [0021] Regarding the aforementioned apparatus comprising the challenge forming device, the response verifying device as well as the optical key, it was found that the reliability of the authentication of the optical key can already be significantly improved when optimizing aspects regarding the optical key itself, although the optical key, once produced, has actually no user-changeable parameters as opposed to the other components of the authentication apparatus.

30 [0022] Thus, according to the invention, the optical key is characterized by a reliable authenticatability when or after being exposed to an external influence, in particular to a physical or chemical stimulus such as a different ambient condition, mechanical stress or chemical contact. This has the advantage that a temporary or prevailing exposure of the optical key to external influences does not change the response of the optical key to a given challenge.

35 [0023] In an embodiment of the apparatus for authenticating an optical key, the optical key is characterized by authenticatability at more than one temperature, preferably at a continuous temperature range, in particular when receiving the challenge formed by the challenge forming device. This has the advantage that the optical key can be used in a wide temperature range, which is essential for practical applications.

40 [0024] In an embodiment of the apparatus for authenticating an optical key, the optical key is characterized by authenticatability after common use such as exposure to touching, clothing or weather. This allows for example that the optical key can be removed from the apparatus in order to be transported or securely stored at a place different from the apparatus. Moreover, this allows the key to be authenticated in different authentication apparatuses of the same type.

45 [0025] In an embodiment of the apparatus for authenticating an optical key, the optical key is characterized by a thermal reliability parameter which is lower than $1/(200,000 \text{ Kelvin})$, preferably lower than $1/(500,000 \text{ Kelvin})$, more preferably lower than $1/(1,000,000 \text{ Kelvin})$, whereat the thermal reliability parameter is the absolute value of one or more summed up temperature coefficients of the optical key, in particular the temperature coefficient of the optical path length $(1/S)(dS/dT)$, where S is the optical path length within the material of the optical key.

50 [0026] The one or more summed up temperature coefficients may for example be selected from the group consisting of the temperature coefficient of a length of the optical key, the temperature coefficient of an area of the optical key, the temperature coefficient of a volume of the optical key and the temperature coefficient of a refractive index of the optical key.

[0027] In other words, the thermal reliability parameter may be defined as the decorrelation speed of the speckle pattern with temperature, in particular the temperature coefficient of the optical path length $(1/S)(dS/dT)$ or its absolute value. The thermal reliability parameter may in particular be positive.

55 [0028] In an embodiment of the apparatus for authenticating an optical key, the optical key comprises at least two different materials and the thermal reliability parameter of each material is lower than $1/(100,000 \text{ Kelvin})$, preferably lower than $1/(200,000 \text{ Kelvin})$, more preferably lower than $1/(500,000 \text{ Kelvin})$.

[0029] In an embodiment of the apparatus for authenticating an optical key, the optical key comprises a ceramic

material, in particular a glass ceramic material. The ceramic material may be a ceramic scattering material preferably with a thermal reliability parameter as indicated above. The glass ceramic material may be for example ZERODUR® K20 or cordierite glass ceramic. Preferably, the optical key comprises or consists of a glass ceramic, in particular a athermal glass ceramic, with at least two different phases, wherein at least one of the phases, for example a crystalline phase, defines a structure which determines the response of the optical key when receiving the challenge formed by the challenge forming device. The phase determining the response may be a physical unclonable function. As glass ceramic, a LAS-system containing lithium-, silicon-, and aluminum-oxides, may be preferred.

[0030] In an embodiment of the apparatus for authenticating an optical key, the optical key contains cordierite, silimanit, cristobalite, Mg-B quartz, mullit and/or eucryptite. The material of the optical key may in particular be a ceramic scattering material containing cordierite, silimanit, cristobalite, Mg-B quartz, mullit and/or eucryptite as crystalline phases, in particular as a physical unclonable function.

[0031] The optical key may also contain AB_2O_8 where A is selected from the group of elements consisting of {Zr, Hf, Zn, Ti, U, TH, Lu} or a mixture of these elements and B is selected from the group of elements consisting of {W, Mo} or mixtures of these elements

[0032] The optical key may also contain CD_2O_7 where C is selected from the group of elements consisting of {Zr, Hf, Zn, Ti, U, TH, Lu, Pu, Np, W, Ce, Sn, Ge, Si} or a mixture of these elements and D is selected from the group of elements consisting of {V,P} or mixtures of these elements

[0033] The optical key may also contain $E_2F_3O_{12}$ where E is selected from the group of elements consisting of {Sc, Y, Lu, Al, Ga, La, "Lanthanoids"} or a mixture of these elements and F is selected from the group of elements consisting of {W, Mo, P}.

[0034] The optical key may also contain GH_3 where G is selected from the group of elements consisting of {Sc, Y, Ba, Mg, Ca, Sr} and H is selected from the group of elements consisting of {F, Cl} or mixtures of these elements including other aliovalent substitutions.

[0035] The optical key may in particular comprise crystalline phases which combine negative thermal expansion with high refractive index.

[0036] In an embodiment of the apparatus for authenticating an optical key, the optical key comprises a material with a tuned scattering property, in particular with a tuned scattering length, preferably of at least 1 and at most 10 micrometer, whereat the material with the tuned scattering property is in particular produced by a method for tuning the scattering property in the manufacture.

[0037] In a preferred embodiment of the apparatus for authenticating an optical key, the optical key comprises a physical unclonable function, in particular such that manufacturing a replica of the optical key is practically unfeasible. The PUF can for example comprise the microscopic arrangement of the crystallites of a ceramic material.

[0038] For practical applications, the reliability of the apparatus comprising the challenge forming device, the response verifying device and the optical key can be further improved by adding special auxiliary equipment to the setup, as described below.

[0039] The apparatus for authenticating an optical key may preferably comprise a fixture for temporal fixation of the optical key, in particular when receiving the challenge formed by the challenge forming device. This allows for a precise positioning an orientation of the optical key and may also provide an option for removing the optical key from the apparatus and reinserting the optical key at the exact same position and orientation.

[0040] The apparatus for authenticating an optical key may further preferably comprise an interpolation device for interpolating between multiple responses of the optical key, in particular obtained at different temperatures for providing an extended authenticatability of the optical key, in particular at an enlarged temperature range. The interpolating device may for example comprise and/or carry out an algorithm to interpolate between the scattering signatures at different temperatures in order to enlarge the temperature range within which a given scatterer can be authenticated.

[0041] The interpolation device and/or the algorithm may also be coupled to the fixation of the key in order to adjust the position and/or orientation of the key. That is, the interpolation device may be designed such as to reposition and/or reorient the optical key. The interpolation device and/or the algorithm may for example also be coupled to a cooling or heating device in order to change the temperature of the optical key, in particular to a value within a predefined temperature range.

[0042] In an embodiment of the apparatus for authenticating an optical key, the number of quanta, e.g., photons, in the challenge formed by the challenge forming device is less than the least possible number of parameters required to unambiguously characterize each setting of the plurality of settings of the challenge forming device. In this case, the authentication may be referred to as quantum secure authentication (QSA). The advantage is that, due to quantum mechanical principles, an adversary can no longer determine the quantum state of the challenge in order to generate the matching response. In other words, the authentication is unconditionally secure.

[0043] The invention further relates to an optical key for an apparatus for optical key authentication, in particular for authentication such as quantum secure authentication.

[0044] The invention further relates to a method for authenticating an optical key by verifying a match of a challenge-

response pair.

[0045] The method for authenticating an optical key comprises a step of forming a challenge by means of a challenge forming device.

[0046] The method for authenticating an optical key further comprises a step of providing a response to the challenge by means of an optical key, which is receptive to the challenge formed by the challenge forming device, when receiving the challenge formed by the challenge forming device, whereat the optical key is characterized by a reliable authenticatability when or after being exposed to an external influence, in particular to a physical or chemical stimulus such as a different ambient condition, mechanical stress or chemical contact.

[0047] The method for authenticating an optical key further comprises a step of verifying if the response provided by the optical key matches the challenge formed by the challenge forming device by means of a response verifying device, which is receptive to the response provided by the optical key.

[0048] The invention further relates to an apparatus for generating a random number from an optical key.

[0049] The apparatus for generating a random number comprises a preferably coherent radiation source for emitting electromagnetic radiation, in particular light.

[0050] The apparatus for generating a random number may optionally comprise a spatial light modulator, which is irradiatable by the radiation emitted by the radiation source, for forming spatially modulated radiation when being irradiated by radiation emitted by the radiation source.

[0051] The apparatus for generating a random number further comprises an optical key, which is irradiatable by the spatially modulated radiation formed by the spatial light modulator or by the radiation emitted by the radiation source, for forming spatially modulated scattered radiation when being irradiated by the spatially modulated radiation formed by the spatial light modulator or by the radiation emitted by the radiation source.

[0052] The apparatus for generating a random number further comprises a detector, which is irradiatable by the spatially modulated scattered radiation formed by the optical key, for providing signals associated to the spatially modulated scattered radiation when being irradiated by the spatially modulated scattered radiation.

[0053] The apparatus for generating a random number further comprises a random number generating device for generating random numbers when receiving the signals provided by the detector, whereat the random number is stable when or after the optical key is exposed to an external influence, in particular a physical or chemical stimulus such as a different ambient condition, mechanical stress or chemical contact.

[0054] In an embodiment of the apparatus for generating a random number, the random number is stable for more than one temperature, preferably for a continuous temperature range, in particular when the optical key is irradiated by the spatially modulated radiation formed by the spatial light modulator. This has the advantage that the optical key can be used in a wide temperature range, which is essential for practical applications.

[0055] In an embodiment of the apparatus for generating a random number, the random number is stable after common use of the optical key such as exposure to touching, clothing or weather. This allows for example that the optical key can be removed from the apparatus in order to be transported or securely stored at a place different from the apparatus. Moreover, this allows the key to be used in different apparatuses for generating a random number.

[0056] In an embodiment of the apparatus for generating a random number, the optical key is characterized by a thermal reliability parameter, in particular as defined above.

[0057] In an embodiment of the apparatus for generating a random number, the optical key comprises a scattering material, in particular as mentioned above, or a ceramic material, for example as indicated above, or a material containing cordierite, sillimanit, cristobalite, Mg-B quartz, mullit and/or eucryptite such as described above.

[0058] In an embodiment of the apparatus for generating a random number, the optical key comprises a material with a tuned scattering property, in particular as outlined above.

[0059] In an embodiment of the apparatus for generating a random number, the optical key comprises a physical unclonable function, in particular as noted above.

[0060] The apparatus for generating a random number may preferably comprise a fixture for temporal fixation of the optical key, in particular when being irradiated by the spatially modulated radiation formed by the spatial light modulator. This allows for a precise positioning an orientation of the optical key and may also provide an option for removing the optical key from the apparatus and reinserting the optical key at the exact same position and orientation.

[0061] The apparatus for generating a random number may further preferably comprise an interpolation device for interpolating between spatially modulated scattered radiation from the optical key obtained at different conditions, in particular at different temperatures, for providing a stable random number, in particular for an enlarged temperature range. The interpolating device may for example comprise and/or carry out an algorithm to interpolate between the scattering signatures of the optical key at different temperatures in order to enlarge the temperature range within which a given scatterer can be used to generate random numbers.

[0062] The interpolation device and/or the algorithm may also be coupled to the fixation of the key in order to adjust the position and/or orientation of the key, in particular as described above. The interpolation device and/or the algorithm may also be coupled to a cooling or heating device in order to change the temperature of the optical key, in particular

as mentioned above.

[0063] The invention further relates to an optical key for an apparatus for generating a random number, in particular for encryption such as one-time pad encryption.

[0064] The invention further relates to a method for generating a random number from an optical key.

[0065] The method for generating a random number comprises a step of emitting electromagnetic radiation, in particular light, by means of a radiation source.

[0066] The method for generating a random number further comprises a step of forming spatially modulated scattered radiation by means of an optical key, which is irradiatable by the radiation emitted by the radiation source, when being irradiated by radiation emitted by the radiation source, whereat the random number is stable when or after the optical key is exposed to an external influence, in particular a physical or chemical stimulus such as a different ambient condition, mechanical stress or chemical contact.

[0067] The method for generating a random number further comprises a step of providing signals associated to the spatially modulated scattered radiation by means of a detector, which is irradiatable by the spatially modulated scattered radiation formed by the optical key, when being irradiated by the spatially modulated scattered radiation.

[0068] The method for generating a random number further comprises a step of generating random numbers by means of a random number generating device, when receiving the signals provided by the detector.

[0069] The invention further relates to using a material with a thermal reliability parameter which is lower than $1/(200,000 \text{ Kelvin})$, preferably lower than $1/(500,000 \text{ Kelvin})$, more preferably lower than $1/(1,000,000 \text{ Kelvin})$, and/or a material as indicated above as an optical key and/or as a physical unclonable function, in particular for authentication such as quantum secure authentication and/or encryption such as one-time pad encryption.

[0070] The invention is explained below in light of examples and drawings, wherein:

Fig. 1: is a schematic drawing of an apparatus for authenticating an optical key,

Fig. 2: is a schematic drawing of an apparatus for generating a random number,

Fig. 3: shows a diagram of an experimental setup for testing properties of speckle patterns,

Fig. 4: shows (a) the decorrelation of speckle pattern from ceramic glass sample during 70 minutes of continuous measurements and (b) a typical image of speckle pattern of ceramic glass,

Fig. 5: shows (a) the displacement of the sample in axial direction by using stage with piezo controller and (b) decorrelation of speckle pattern from ceramic glass sample measured during displacement with the constant temperature,

Fig. 6: shows axial shift of the sample position during heating from 21 degrees to 43 degrees,

Fig. 7: shows the time dependence of decorrelation of speckle pattern (thin line) and temperature (thick line) for ceramic glass ZERODUR® K20 from a first measurement (a) and from a second measurement (b) on the same sample,

Fig. 8: shows the time dependence of decorrelation of speckle pattern (thin line) and temperature (thick line) for LZS ceramic glass,

Fig. 9: shows (a) the time dependence of decorrelation of speckle pattern (thin line) and temperature (thick line) for standard ground glass diffuser and (b) changes in temperature in degrees as a function of decorrelation (in per cent), wherein dots are experimental values and the dashed line is a line approximation with parameters as indicated in the table below,

Fig. 10: shows the decorrelation of a speckle pattern as a function of temperature for three different materials used for an optical key.

[0071] Referring to Fig. 1, the optical key authentication apparatus 10 comprises a laser 12 for emitting coherent light 14, which strikes on a SLM 15 of a challenge forming device 16. The SLM 15 introduces challenge information, e.g., from a challenge-response pair database to which the challenge forming device 16 may be coupled, into the light beam 14. Thus the challenge forming device forms a challenge 18, which passes through a beam splitter 20 and strikes on an optical key 22, which is firmly mounted in a fixation 24.

[0072] The optical key 22, comprised in the apparatus 10, provides a response 26 to the challenge 18, which is reflected

back onto the beam splitter 20 and coupled out onto a SLM 28 of a response verifying device 30. The SLM 28, which is adjusted to a setting which belongs to the setting of the SLM 15 of the challenge forming device 16, introduces response information, e.g., from the aforementioned challenge-response pair database, into the response 26 in order to cancel the spatial modulations, provided the optical key 22 acts as expected. In other words, the SLM 28 is set to a setting, which revokes the spatial modulations of the response of the optical key 22 to the given challenge 18 formed by the SLM 15.

[0073] The light pulse 32 can now be focused, e.g., by a lens 34 through a pinhole plane 36 onto a detector 40. The detector 40 of the response verifying device 30 may, e.g., count the number of photons in the incident light pulse 38. If the spatial modulations have been revoked successfully, i.e., if the optical key is correct, the detector 40 counts more photons than in the case where the optical key is incorrect. In the latter case, the spatial modulations of the response cannot be cancelled out such that focusing the light pulse 32 fails.

[0074] Referring to Fig. 2, the optical key random number generation device 50 also comprises a coherent light source 54 for emitting coherent light 54 passing through a spatial light modulator 56 leading to spatially modulated light 58. The spatially modulated light 58 hits on an optical key 62, which is fixed to a key mount 60, leading to spatially modulated scattered light 64. The spatially modulated scattered light 64 strikes on a detector 66, which detects the speckle pattern of the spatially modulated scattered light 64. Based on the speckle pattern on the detector plane, the detector 66 provides electric signals through a link 68 to a random number generator 70.

[0075] The introduction of spatial modulations using the spatial light modulator 56 acquires its meaning, when implementing a one-time pad encryption, where for example two optical keys are used, cf. e.g., US 2013/0243187 A1.

[0076] While the optical key 22 in the example of Fig. 1 operates in reflection mode, the optical key 62 in the example of Fig. 2 works in passage mode. However, this may also be configured vice versa, respectively.

[0077] Referring to Fig. 1 and 2, the optical keys 22, 62 are manufactured from a strongly scattering media. The strongly scattering medium comprises random scatterers and thus has a unique scattering signature, when illuminated. The speckle pattern of the illuminated strongly scattering object contains a combination of coherent and incoherent scattering contributions, so that slight changes in the scattering medium have dramatic consequences for the speckle pattern. This attribute, together with the fact that copying of optical fields becomes impossible in the low photon number limit, makes strongly scattering media an ideal and robust key for secure encryption.

[0078] Moreover, the optical keys 22, 62 are volumetric scatterers. Optical keys consisting of three-dimensional media are much more secure than keys made out of two-dimensional materials such as paper.

[0079] Referring to Fig. 3, an experimental setup for testing properties of speckle patterns is illustrated. Beam splitters are denoted as BS, a polarizing beam splitter as PBS, a thermoresistor as TR, an objective as obj and a half-wave plate as $\lambda/2$.

[0080] The setup has been used to experimentally test speckle patterns of different glass and ceramic based scattering materials in the wide temperature range. In what follows, it is detailed that it could be shown that special ceramic samples are stable (less than 1% decorrelation) within a temperature range from 20 to 30 °C.

[0081] Continuous wave output of He-Ne laser 100 with a wavelength of 633 nm is employed to produce speckle picture from different scattering samples. Laser radiation is focused to the sample 102 with microscope objective 104 (10x, NA = 0.25). Scattering light is collected in backward direction with the help of the same objective 104. Standard CCD camera 106 from Allient is used to visualize speckle pattern 108. Heating is performed by using an external heater which is brought close to the sample (approximately 1 cm distance).

[0082] A Michelson interferometer 110 is used for measuring displacement of the sample in axial direction with resolution better than 100 nm. A typical interference pattern 112 is sketched in left part of the illustration. Temperature control is performed by measuring changes in resistivity of pt100 resistance temperature detector 114 attached to the surface of the sample with thermo conductive glue. Accuracy of the Multimeter 116 allows to measure temperature with high resolution. Experiments were made on different samples: ground glass diffusers and ceramic glasses.

[0083] In a control series of experiments (calibration measurements), long-term variations in the speckle pictures without additional heating have been quantified. Decorrelation (D) as a function of time was calculated with the following formula:

$$D(t) = \left(1 - \frac{\sum R_{t,0}}{\sum R_{0,0}}\right) 100\%$$

[0084] Where R_{t_1,t_2} - cross correlation between images obtained at the moment t_1 and t_2 . Changes in correlations of speckle patterns during more than 1 hour of measurements are presented at the Fig 4(a). Average decorrelation during 1 hour was 0.5 % with the standard deviation of 0.2 %. It is seen that all data points are within the range of 1.2%. Temperature measured with the help of thermistor during the same time was $21.15 \pm 0.04^\circ$. Laser power was stable within 0.2%. Position of sample was stable within 0.1 μm . Typical image of speckle pattern of ceramic glass is presented in Fig. 4(b).

[0085] An influence of small sample displacement on the speckle pattern decorrelation was also measured. The sample was displaced in controllable way with the 3D Piezo stage in axial direction in the range from 0 to 2.75 μm and simultaneously measured changes in position with the help of Michelson interferometer, as shown in Fig 5(a). Temperature was constant. So these measurements can be compared with decorrelation of speckle pattern. The result is presented on the Fig 5(b), wherein the experimental decorrelation data and an area of 1.2% (horizontal lines) are shown. It is seen that despite of the movements of the sample decorrelation still lie within an estimated error area of 1.2%.

[0086] From minute 5 to 9 in Fig. 5b it is also seen that the displacement of the sample giving rise to small oscillations which, however, also do not lead to large changes in absolute value of decorrelation.

[0087] Furthermore, the displacement of the sample during the heating from 21° to 43° was checked. Such temperature changes cause shift in position of the sample less than 2 μm as can be seen from Fig. 6. This displacement, as was shown in the previous measurements (Fig. 5), causes no noticeable changes in decorrelation leading only to oscillations near the mean value. Thus, all changes in decorrelation above an error value are due to internal changes in the sample.

[0088] The results of the calibration measurements, as discussed so far, were presented for ceramic glass sample. It is noted that the character of such data was the same for all kind of samples.

[0089] In what follows, results of measurements are presented for ZERODUR® K20 (as first sample), a LZS-1/6C glass ceramic (as second sample) and a ground glass (as third sample).

[0090] As a first sample, ZERODUR® K20 glass ceramic has been used. This sample contains keatite solid-solution crystals: $\text{LiAlSi}_2\text{O}_6$, some amount of Zn and P additions (2 μm size) and less than 5 wt% of ZrTiO_4 crystals (5 nm size). Any residual glass preferably is quite low in content, but would be enriched in Al_2O_3 and SiO_2 .

[0091] Fig. 7 show results of simultaneous measurements of decorrelation of speckle pattern (thin line) and temperature (thick line) for ZERODUR® K20 ceramic glass. Fig. 7(a) and Fig. 7(b) present data from two different experiments on the same sample. Horizontal lines show an error area of $\pm 0.6\%$ estimated in previous calibration measurements.

[0092] As can be seen, the significant changes in decorrelation appear only when the temperature increases more than 10 degrees. Heating by 20 degrees leads to changes only in 1.6%. Well resolved oscillations occur due to small shifting of the sample as have been shown before in Fig. 5(b).

[0093] As a second sample, a LZS glass-ceramic (LZS-1/6C) is used. The sample comprises nearly 40 wt% residual glass, the main crystal phases are a complex Li-Zn-silicate phase (37 wt%) of imprecise stoichiometry along with a considerable amount of cristobalite (nearly pure SiO_2) at about 25 wt%.

[0094] Simultaneous measurements of decorrelation of speckle pattern (thin line) and temperature (thick line) for LZS ceramic glass are presented in Fig. 8. Horizontal lines show an error area of $\pm 0.6\%$ estimated in previous measurements. In this case, heating by 10 degrees leads to changes in approximately 2%. Well resolved oscillations occur due to small axial shifting of the sample as have been shown before.

[0095] As a third sample, a standard glass diffuser is used. Measurements of decorrelation of speckle pattern (thin line) and temperature (thick line) for standard ground glass diffuser are presented in Fig. 9(a). It is seen that the ground glass diffuser is more sensitive to temperature changes. Temperature changes by less than half degree induce significant increase per cent of decorrelation. Changes in temperature in degrees as a function of decorrelation (in per cent) are presented in Fig. 9(b), wherein dots are experimental values and the dashed line is a line approximation with parameters as indicated in the table below Fig. 9(b).

[0096] Referring to Fig. 10 the temperature dependence of the speckle pattern provided by optical keys manufactured from different scattering media as outlined before is shown. The data is extracted from data presented in Figures 7-9 and normalized to zero on the temperature scale and also to zero on the decorrelation scale for comparison. The dashed area 86 represents a long-term errors area estimated in the calibration measurement shown in Fig. 4(a). Solid lines are linear approximations of the experimental data ($D=\alpha\Delta T$, where D are changes in decorrelation in units (non per cent), ΔT are changes in temperature in degrees and α is the linear thermal expansion coefficient in K^{-1}).

[0097] The scattering signature 80 corresponds to an optical key made from ground glass. As can be seen, already a slight temperature change of a few degrees leads to a dramatic decorrelation of the speckle pattern.

[0098] In fact, it has been found that most scattering materials show a speckle pattern which strongly changes with temperature. It has been found that the reason for this is that in most materials thermal expansion is present in addition to a change of the refractive index n as a function of temperature. In other words both, the linear thermal expansion

coefficient $\alpha = \frac{1}{L} \frac{dL}{dT}$ as well as the thermo-optic coefficient $\tau_n = \frac{1}{n} \frac{dn}{dT}$ is non-negligible.

[0099] In most scattering materials, even a few degrees change in temperature lead to a complete decorrelation of the scattering signature and the properties of a scattering key are lost. This problem has been experimentally verified, e.g., by using TiO_2 paste on glass as a scattering medium or by using strongly scattering polymers, and thus constitutes a real technical issue.

[0100] In order to solve this problem, the optical key 22, 62 is preferably manufactured from a material with a near-

athermal scattering signature. In other words, the PUF is built to be applicable in a wide temperature range.

[0101] Referring to Fig. 10, two glass ceramic systems have been used and compared to the scattering signature 80 of ground glass ($\alpha = 27 \times 10^{-6} \text{ K}^{-1}$). The scattering signature 82 corresponds to a LZS glass ceramic ($\alpha = 2.1 \times 10^{-6} \text{ K}^{-1}$) and the scattering signature 84 corresponds to ZERODUR® K20 ($\alpha = 0.9 \times 10^{-6} \text{ K}^{-1}$). The optical key 22, 62 may thus in particular comprise a glass ceramic. The material of the optical key may in particular comprise LZS and/or ZERODUR® K20. Moreover, the material may in particular have a thermal expansion coefficient of $\alpha < 2.5 \times 10^{-6} \text{ K}^{-1}$, preferably $\alpha < 1.0 \times 10^{-6} \text{ K}^{-1}$.

[0102] Decorrelation of the speckle patterns are affected by changes in the optical path length. The optical path length, $S=L*n$, in a homogeneous medium is defined as the product of the geometrical length, L, with the refractive index, n. The thermal coefficient of the optical path is then:

$$\frac{1}{S} \frac{dS}{dT} = \frac{1}{L} \frac{d(Ln)}{dT} = \frac{1}{L} \frac{dL}{dT} + \frac{1}{n} \frac{dn}{dT} = \alpha + \tau_n$$

which may be an expression of a thermal reliability parameter of an optical key.

[0103] The decorrelation speed of the speckle pattern with temperature is expected to be proportional to $(1/S)(dS/dT)$. By denoting $(1/S)(dS/dT)=\beta$ and using $D=\alpha\Delta T$, one can write $(1/S)(dS/dD)=(\beta/\alpha)$. After integration: $S(D)=S(0)\exp(D\beta/\alpha)$ and $D\beta/\alpha=\ln(1+\Delta L/L)$, where $\Delta L=L(D)-L(0)$; $\Delta L/L \ll 1$. Thus, $D\beta/\alpha$ can be approximated as $\Delta L/L$; and $D=(\alpha/(\beta L))\Delta L$. Therefore, decorrelation speed as a function of temperature depends on sample properties described by β (sum of linear thermal expansion coefficient and thermo-optic coefficient) and average light path length inside the sample, which is determined by sample properties such as mean free path as well as parameters of illumination. For example, L will be significantly larger in the transmission geometry in comparison with reflection geometry in the case of the same sample. Hence, for minimization of decorrelation speed a decrease of β as well as decrease average light path length inside the sample by adjusting experimental geometry is beneficial.

[0104] The optical key comprises in particular a material for which α is smaller than $5.0 \times 10^{-6} \text{ K}^{-1}$ and/or τ_n is smaller than $5.0 \times 10^{-6} \text{ K}^{-1}$. Preferably, the key comprises a material for which $\alpha + \tau_n$ is smaller than $5.0 \times 10^{-6} \text{ K}^{-1}$. This has the advantage that the scattering properties of the material are less dependent of temperature, i.e., exhibit a near-athermal scattering behavior. This means a wave front propagates undisturbed. However, manufacturing a material for which both α and τ_n become small is rather difficult.

[0105] The same invariance of the scattering properties can be achieved by matching the thermal expansion of a material to be opposite to that of the temperature coefficient of the refractive index, so that they compensate each other, which gives much more opportunity to make such materials. Thus, the optical key in particular comprises a material for which α and τ_n at least partially cancel each other. More preferably, the key comprises a material for which the absolute value $|\alpha + \tau_n|$ is smaller than $5.0 \times 10^{-6} \text{ K}^{-1}$.

[0106] In a strongly scattering medium, the situation is more complicated in that scattering signatures for at least two different phases, e.g., crystal(s) and residual glass, with different refractive indices are needed for proper characterization of the composite material. In general, the constituent phases have their individual thermal expansions and their individual thermal coefficients for the refractive indices. In such a situation, the weighted sum of the α and the τ_n of the materials can give an estimate of their combined effect, neglecting higher order corrections. Hence, the optical key in particular comprises a material for which $|A + T_n|$ is smaller than $5.0 \times 10^{-6} \text{ K}^{-1}$, where A is the weighted sum of the α of the phases of the material and T is the weighted sum of the τ_n of the phases.

[0107] Using scattering materials with close to zero thermal expansion and not too large τ_n values leads to small decorrelation as a function of temperature.

The advantage of these materials is that changes in temperature have considerably less effect on the speckle pattern of the scattering object, while when using normal materials, slight changes in temperature change the speckle pattern of the strongly scattering object, thereby also changing the scattering signature. In other word, by using a strongly scattering material with a near-athermal scattering signature, the optical key 22, 62 can be produced such that it can be used in a wide temperature range. Such athermal behavior is particularly beneficial for practical applications.

[0108] Using a strongly scattering, durable material with a small thermal expansion as a key for secure authentication offers the possibility of a robust and practical applicable authentication technique for numerous applications.

Claims

1. An apparatus for authenticating an optical key by verifying a match of a challenge-response pair comprising:

- a challenge forming device for forming a challenge,

- an optical key, which comprises scattering material and is receptive to the challenge formed by the challenge forming device, for providing a response to the challenge when receiving the challenge formed by the challenge forming device,
- a response verifying device, which is receptive to the response provided by the optical key, for verifying if the response provided by the optical key matches the challenge formed by the challenge forming device,
- whereat the optical key is **characterized by** a reliable authenticatability when or after being exposed to an external influence, in particular to a physical or chemical stimulus such as a different ambient condition, mechanical stress or chemical contact.
2. An apparatus for authenticating an optical key according to any one of the preceding claims whereat the optical key is **characterized by** authenticatability at more than one temperature, preferably at a continuous temperature range, in particular when receiving the challenge formed by the challenge forming device.
 3. An apparatus for authenticating an optical key according to any one of the preceding claims whereat the optical key is **characterized by** authenticatability after common use such as exposure to touching, clothing or weather.
 4. An apparatus for authenticating an optical key according to any one of the preceding claims whereat the optical key is **characterized by** a thermal reliability parameter being lower than $1/(200,000 \text{ Kelvin})$, preferably lower than $1/(500,000 \text{ Kelvin})$, more preferably lower than $1/(1,000,000 \text{ Kelvin})$, whereat the thermal reliability parameter is the absolute value of one or more summed up temperature coefficients of the optical key, in particular the temperature coefficient of the optical path length $(1/S)(dS/dT)$.
 5. An apparatus for authenticating an optical key according to the preceding claim whereat the one or more summed up temperature coefficients are selected from the group consisting of the temperature coefficient of a length of the optical key, the temperature coefficient of an area of the optical key, the temperature coefficient of a volume of the optical key and the temperature coefficient of a refractive index of the optical key.
 6. An apparatus for authenticating an optical key according to any one of the preceding claims whereat the optical key comprises at least two different materials and the thermal reliability parameter of each material is lower than $1/(100,000 \text{ Kelvin})$, preferably lower than $1/(200,000 \text{ Kelvin})$, more preferably lower than $1/(500,000 \text{ Kelvin})$.
 7. An apparatus for authenticating an optical key according to any one of the preceding claims whereat the optical key comprises a ceramic material, in particular a glass ceramic material, with at least two different phases, wherein at least one of the phases defines a structure which determines the response of the optical key when receiving the challenge formed by the challenge forming device.
 8. An apparatus for authenticating an optical key according to any one of the preceding claims whereat the optical key contains cordierite, silimanit, cristobalite, Mg-B quartz, mullit, eucryptite, AB_2O_8 where A is selected from the group of elements consisting of {Zr, Hf, Zn, Ti, U, TH, Lu} or a mixture of these elements and B is selected from the group of elements consisting of {W, Mo} or mixtures of these elements, CD_2O_7 where C is selected from the group of elements consisting of {Zr, Hf, Zn, Ti, U, TH, Lu, Pu, Np, W, Ce, Sn, Ge, Si} or a mixture of these elements and D is selected from the group of elements consisting of {V, P} or mixtures of these elements, $E_2F_3O_{12}$ where E is selected from the group of elements consisting of {Sc, Y, Lu, Al, Ga, La, "Lanthanoids"} or a mixture of these elements and F is selected from the group of elements consisting of {W, Mo, P} and/or GH_3 where G is selected from the group of elements consisting of {Sc, Y, Ba, Mg, Ca, Sr} and H is selected from the group of elements consisting of {F, Cl} or mixtures of these elements including other aliovalent substitutions.
 9. An apparatus for authenticating an optical key according to any one of the preceding claims whereat the optical key comprises a material with a tuned scattering property, in particular with a tuned scattering length, preferably of at least 1 and at most 10 micrometer, whereat the material with the tuned scattering property is in particular produced by a method for tuning the scattering property in the manufacture.
 10. An apparatus for authenticating an optical key according to the preceding claim whereat the optical key comprises a physical unclonable function, in particular such that manufacturing a replica of the optical key is practically unfeasible.
 11. An apparatus for authenticating an optical key according to any one of the preceding claims comprising:

- a fixture for temporal fixation of the optical key, in particular when receiving the challenge formed by the challenge forming device and/or
- an interpolation device for interpolating between multiple responses of the optical key, in particular obtained at different temperatures, for providing an extended authenticatability of the optical key, in particular at an enlarged temperature range.

12. An apparatus for authenticating an optical key according to any one of the preceding claims comprising at least one of the following features:

- a radiation source for emitting radiation comprising quanta, in particular for emitting electromagnetic radiation comprising photons,
- the challenge forming device is irradiatable by the radiation emitted by the radiation source and the challenge forming device is adapted for forming the challenge when being irradiated by radiation emitted by the radiation source,
- the challenge forming device is adjustable such that the challenge forming device can adopt one of a plurality of settings,
- the number of quanta in the challenge formed by the challenge forming device is less than the least possible number of parameters required to unambiguously characterize each setting of the plurality of settings of the challenge forming device,
- the response verifying device is adjustable in the same manner as the challenge forming device, whereat each setting of the response verifying device matches one setting of the challenge forming device,
- the challenge forming device and/or the response verifying device comprises a spatial light modulator.

13. An optical key for an apparatus according to any one of the preceding claims, in particular for authentication such as quantum secure authentication.

14. A method for authenticating an optical key by verifying a match of a challenge-response pair comprising the following steps:

- forming a challenge by means of a challenge forming device,
- providing a response to the challenge by means of an optical key, which is receptive to the challenge formed by the challenge forming device, when receiving the challenge formed by the challenge forming device,
- verifying if the response provided by the optical key matches the challenge formed by the challenge forming device by means of a response verifying device, which is receptive to the response provided by the optical key,
- whereat the optical key is **characterized by** a reliable authenticatability when or after being exposed to an external influence, in particular to a physical or chemical stimulus such as a different ambient condition, mechanical stress or chemical contact.

15. An apparatus for generating a random number from an optical key comprising:

- a radiation source for emitting electromagnetic radiation, in particular light,
- an optical key, which is irradiatable by the radiation emitted by the radiation source, for forming spatially modulated scattered radiation when being irradiated by radiation emitted by the radiation source,
- a detector, which is irradiatable by the spatially modulated scattered radiation formed by the optical key, for providing signals associated to the spatially modulated scattered radiation when being irradiated by the spatially modulated scattered radiation,
- a random number generating device for generating random numbers when receiving the signals provided by the detector,
- whereat the random number is stable when or after the optical key is exposed to an external influence, in particular a physical or chemical stimulus such as a different ambient condition, mechanical stress or chemical contact.

16. An apparatus for generating a random number from an optical key according to claim 15 whereat the random number is stable for more than one temperature, preferably for a continuous temperature range, in particular when the optical key is irradiated by the spatially modulated radiation formed by the spatial light modulator.

17. An apparatus for generating a random number from an optical key according to claim 15 or 16 whereat the random number is stable after common use of the optical key such as exposure to touching, clothing or weather.

18. An apparatus for generating a random number from an optical key according to claim 15 to 17 whereat the optical key is **characterized by** a feature according to any one of the claims 4 to 10.

5 19. An apparatus for generating a random number from an optical key according to any one of the claims 15 to 18 comprising:

- a fixture for temporal fixation of the optical key, in particular when being irradiated by the spatially modulated radiation formed by the spatial light modulator and/or
- 10 - an interpolation device for interpolating between spatially modulated scattered radiation from the optical key obtained at different conditions, in particular at different temperatures, for providing a stable random number, in particular for an enlarged temperature range.

15 20. An optical key for an apparatus according to any one of the claims 15 to 19, in particular for encryption such as one-time pad encryption.

21. A method for generating a random number from an optical key comprising the following steps:

- emitting electromagnetic radiation, in particular light, by means of a radiation source,
- 20 - forming spatially modulated scattered radiation by means of an optical key, which is irradiatable by the radiation emitted by the radiation source, when being irradiated by radiation emitted by the radiation source,
- providing signals associated to the spatially modulated scattered radiation by means of a detector, which is irradiatable by the spatially modulated scattered radiation formed by the optical key, when being irradiated by the spatially modulated scattered radiation,
- 25 - generating random numbers by means of a random number generating device, when receiving the signals provided by the detector,
- whereat the random number is stable when or after the optical key is exposed to an external influence, in particular a physical or chemical stimulus such as a different ambient condition, mechanical stress or chemical contact.

30 22. Using a material with a thermal reliability parameter according to claim 4 or 5 and/or a material according to any one of the claims 6 to 9 as an optical key and/or physical unclonable function, in particular for authentication such as quantum secure authentication and/or encryption such as one-time pad encryption.

35 **Amended claims in accordance with Rule 137(2) EPC.**

1. An apparatus (10) for authenticating an optical key (22) by verifying a match of a challenge-response pair comprising:

- 40 - a challenge forming device (16) for forming a challenge (18),
- an optical key (22), which comprises scattering material and is receptive to the challenge (18) formed by the challenge forming device (16), for providing a response (26) to the challenge (18) when receiving the challenge (18) formed by the challenge forming device (16),
- 45 - a response verifying device (30), which is receptive to the response (26) provided by the optical key (22), for verifying if the response (26) provided by the optical key (22) matches the challenge (18) formed by the challenge forming device (16),
- whereat the optical key (22) is **characterized by** a thermal reliability parameter being lower than 1/(200,000 Kelvin) whereat the thermal reliability parameter is the absolute value of one or more summed up temperature coefficients of the optical key (22).

50 2. An apparatus (10) for authenticating an optical key (22) according to any one the preceding claims whereat the optical key (22) is **characterized by** authenticatability at more than one temperature, preferably at a continuous temperature range, in particular when receiving the challenge formed by the challenge forming device.

55 3. An apparatus (10) for authenticating an optical key (22) according to any one of the preceding claims whereat the optical key (22) is **characterized by** authenticatability after common use such as exposure to touching, clothing or weather.

4. An apparatus (10) for authenticating an optical key (22) according to any one of the preceding claims whereat the

optical key (22) is **characterized by** a thermal reliability parameter being lower than $1/(500,000 \text{ Kelvin})$, preferably lower than $1/(1,000,000 \text{ Kelvin})$, whereat the thermal reliability parameter is in particular the temperature coefficient of the optical path length $(1/S)(dS/dT)$.

- 5 **5.** An apparatus (10) for authenticating an optical key (22) according to any one of the preceding claims whereat the one or more summed up temperature coefficients are selected from the group consisting of the temperature coefficient of a length of the optical key (22), the temperature coefficient of an area of the optical key (22), the temperature coefficient of a volume of the optical key (22) and the temperature coefficient of a refractive index of the optical key (22).
- 10 **6.** An apparatus (10) for authenticating an optical key (22) according to any one of the preceding claims whereat the optical key (22) comprises at least two different materials and the thermal reliability parameter of each material is lower than $1/(100,000 \text{ Kelvin})$, preferably lower than $1/(200,000 \text{ Kelvin})$, more preferably lower than $1/(500,000 \text{ Kelvin})$.
- 15 **7.** An apparatus (10) for authenticating an optical key (22) according to any one of the preceding claims whereat the optical key (22) comprises a ceramic material, in particular a glass ceramic material, with at least two different phases, wherein at least one of the phases defines a structure which determines the response of the optical key (22) when receiving the challenge (18) formed by the challenge forming device (16) .
- 20 **8.** An apparatus (10) for authenticating an optical key (22) according to any one of the preceding claims whereat the optical key (22) contains cordierite, silimanit, cristobalite, Mg-B quartz, mullit, eucryptite, AB_2O_8 where A is selected from the group of elements consisting of {Zr, Hf, Zn, Ti, U, TH, Lu} or a mixture of these elements and B is selected from the group of elements consisting of {W, Mo} or mixtures of these elements, CD_2O_7 where C is selected from the group of elements consisting of {Zr, Hf, Zn, Ti, U, TH, Lu, Pu, Np, W, Ce, Sn, Ge, Si} or a mixture of these elements and D is selected from the group of elements consisting of {V,P} or mixtures of these elements, $E_2F_3O_{12}$ where E is selected from the group of elements consisting of {Sc, Y, Lu, Al, Ga, La, "Lanthanoids"} or a mixture of these elements and F is selected from the group of elements consisting of {W, Mo, P} and/or GH_3 where G is selected from the group of elements consisting of {Sc, Y, Ba, Mg, Ca, Sr} and H is selected from the group of elements consisting of {F, Cl} or mixtures of these elements including other aliovalent substitutions.
- 25 **9.** An apparatus (10) for authenticating an optical key (22) according to any one of the preceding claims whereat the optical key (22) comprises a material with a tuned scattering property, in particular with a tuned scattering length, preferably of at least 1 and at most 10 micrometer, whereat the material with the tuned scattering property is in particular produced by a method for tuning the scattering property in the manufacture.
- 30 **10.** An apparatus (10) for authenticating an optical key (22) according to the preceding claim whereat the optical key (22) comprises a physical unclonable function, in particular such that manufacturing a replica of the optical key is practically unfeasible.
- 35 **11.** An apparatus (10) for authenticating an optical key (22) according to any one of the preceding claims comprising:
- a fixture (24) for temporal fixation of the optical key, in particular when receiving the challenge (18) formed by the challenge forming device (16) and/or
 - an interpolation device for interpolating between multiple responses of the optical key (22), in particular obtained at different temperatures, for providing an extended authenticatability of the optical key (22), in particular at an enlarged temperature range.
- 40 **12.** An apparatus (10) for authenticating an optical key (22) according to any one of the preceding claims comprising at least one of the following features:
- 45 - a radiation source (12) for emitting radiation (14) comprising quanta, in particular for emitting electromagnetic radiation comprising photons,
- 50 - the challenge forming device (16) is irradiatable by the radiation (14) emitted by the radiation source (12) and the challenge forming (16) device is adapted for forming the challenge (18) when being irradiated by radiation (14) emitted by the radiation source (12),
- 55 - the challenge forming device (16) is adjustable such that the challenge forming device (16) can adopt one of a plurality of settings,
- the number of quanta in the challenge (18) formed by the challenge forming device (16) is less than the least

possible number of parameters required to unambiguously characterize each setting of the plurality of settings of the challenge forming device (16),

- the response verifying device (30) is adjustable in the same manner as the challenge forming device (16), whereat each setting of the response verifying device (30) matches one setting of the challenge forming device (16),

- the challenge forming device (16) and/or the response verifying device (30) comprises a spatial light modulator (15, 28).

13. An optical key (22) for an apparatus (10) according to any one of the preceding claims, in particular for authentication such as quantum secure authentication.

14. A method for authenticating an optical key (22) by verifying a match of a challenge-response pair comprising the following steps:

- forming a challenge (18) by means of a challenge forming device (16),

- providing a response (26) to the challenge (18) by means of an optical key (22), which is receptive to the challenge (18) formed by the challenge forming device (16), when receiving the challenge (18) formed by the challenge forming device (16),

- verifying if the response (26) provided by the optical key (22) matches the challenge (18) formed by the challenge forming device (16) by means of a response verifying device (30), which is receptive to the response (26) provided by the optical key (22),

- whereat the optical key (22) is **characterized by** a thermal reliability parameter being lower than 1/(200,000 Kelvin) whereat the thermal reliability parameter is the absolute value of one or more summed up temperature coefficients of the optical key (22).

15. An apparatus (50) for generating a random number from an optical key (62) comprising:

- a radiation source (52) for emitting electromagnetic radiation (54), in particular light,

- an optical key (62), which is irradiatable by the radiation emitted by the radiation source, for forming spatially modulated scattered radiation (64) when being irradiated by radiation emitted by the radiation source,

- a detector (66), which is irradiatable by the spatially modulated scattered radiation (64) formed by the optical key (62), for providing signals associated to the spatially modulated scattered radiation (64) when being irradiated by the spatially modulated scattered radiation (64),

- a random number generating device (70) for generating random numbers when receiving the signals provided by the detector,

- whereat the optical key (62) is **characterized by** a thermal reliability parameter being lower than 1/(200,000 Kelvin) whereat the thermal reliability parameter is the absolute value of one or more summed up temperature coefficients of the optical key (62).

16. An apparatus (50) for generating a random number from an optical key (62) according to claim 15 whereat the random number is stable for more than one temperature, preferably for a continuous temperature range, in particular when the optical key (62) is irradiated by the spatially modulated radiation (58) formed by the spatial light modulator (56).

17. An apparatus (50) for generating a random number from an optical key (62) according to claim 15 or 16 whereat the random number is stable after common use of the optical key (62) such as exposure to touching, clothing or weather.

18. An apparatus (50) for generating a random number from an optical key (62) according to claim 15 to 17 whereat the optical key (62) is **characterized by** a feature according to any one of the claims 4 to 10.

19. An apparatus (50) for generating a random number from an optical key (62) according to any one of the claims 15 to 18 comprising:

- a fixture (60) for temporal fixation of the optical key (62), in particular when being irradiated by the spatially modulated radiation (58) formed by the spatial light modulator (56) and/or

- an interpolation device for interpolating between spatially modulated scattered radiation (64) from the optical key (62) obtained at different conditions, in particular at different temperatures, for providing a stable random

number, in particular for an enlarged temperature range.

20. An optical key (62) for an apparatus (50) according to any one of the claims 15 to 19, in particular for encryption such as one-time pad encryption.

5

21. A method for generating a random number from an optical key (62) comprising the following steps:

- emitting electromagnetic radiation (54), in particular light, by means of a radiation source (52),
- forming spatially modulated scattered radiation (64) by means of an optical key (62), which is irradiatable by the radiation emitted by the radiation source, when being irradiated by radiation emitted by the radiation source,
- providing signals associated to the spatially modulated scattered radiation (64) by means of a detector (66), which is irradiatable by the spatially modulated scattered radiation (64) formed by the optical key (62), when being irradiated by the spatially modulated scattered radiation (64),
- generating random numbers by means of a random number generating device (70), when receiving the signals provided by the detector (66),
- whereat the optical key (62) is **characterized by** a thermal reliability parameter being lower than $1/(200,000 \text{ Kelvin})$ whereat the thermal reliability parameter is the absolute value of one or more summed up temperature coefficients of the optical key (62).

10

15

20

22. Using a material with a thermal reliability parameter according to claim 1, 15, 4 or 5 and/or a material according to any one of the claims 6 to 9 as an optical key (22, 62) and/or physical unclonable function, in particular for authentication such as quantum secure authentication and/or encryption such as one-time pad encryption.

25

30

35

40

45

50

55

Fig. 1

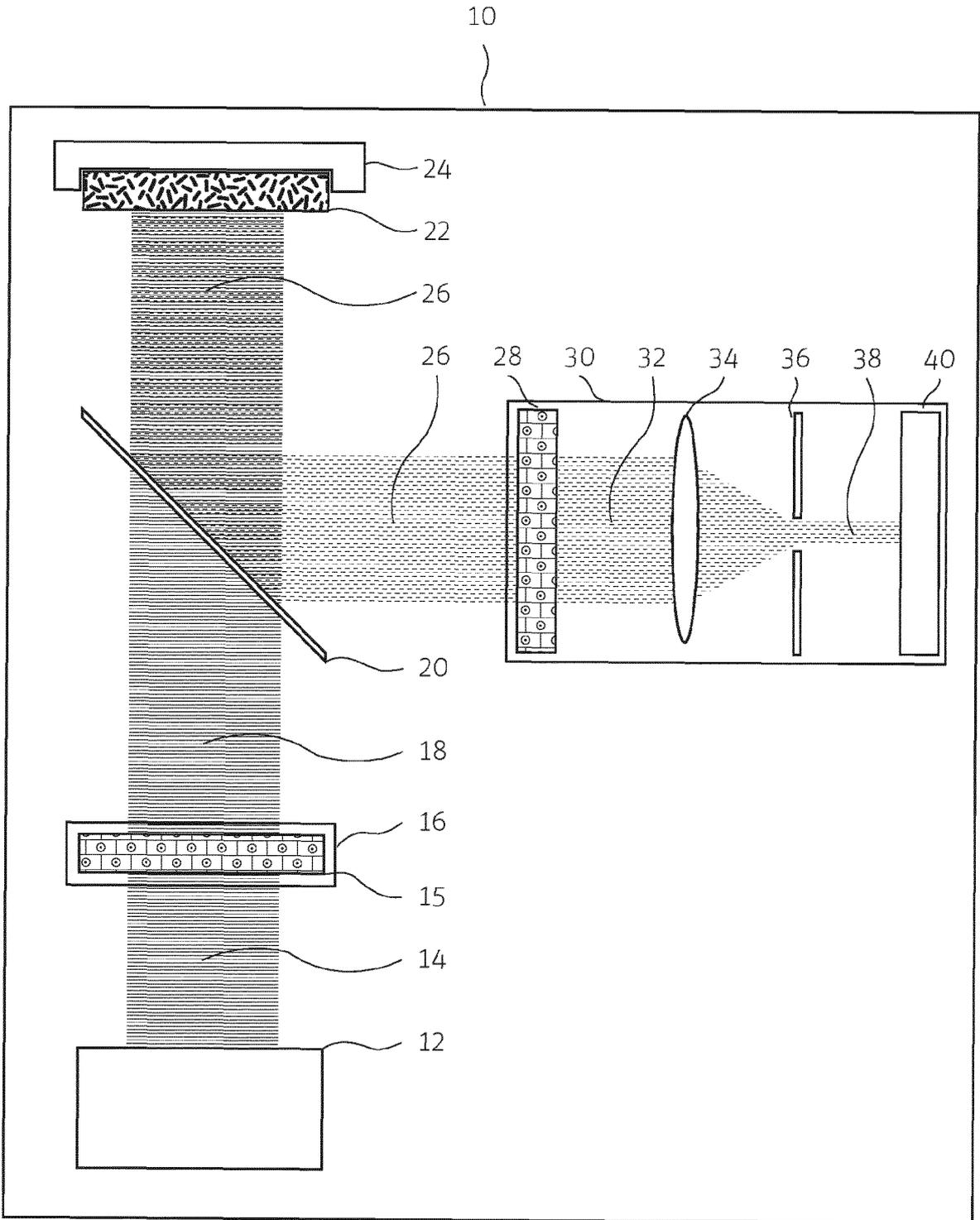


Fig. 2

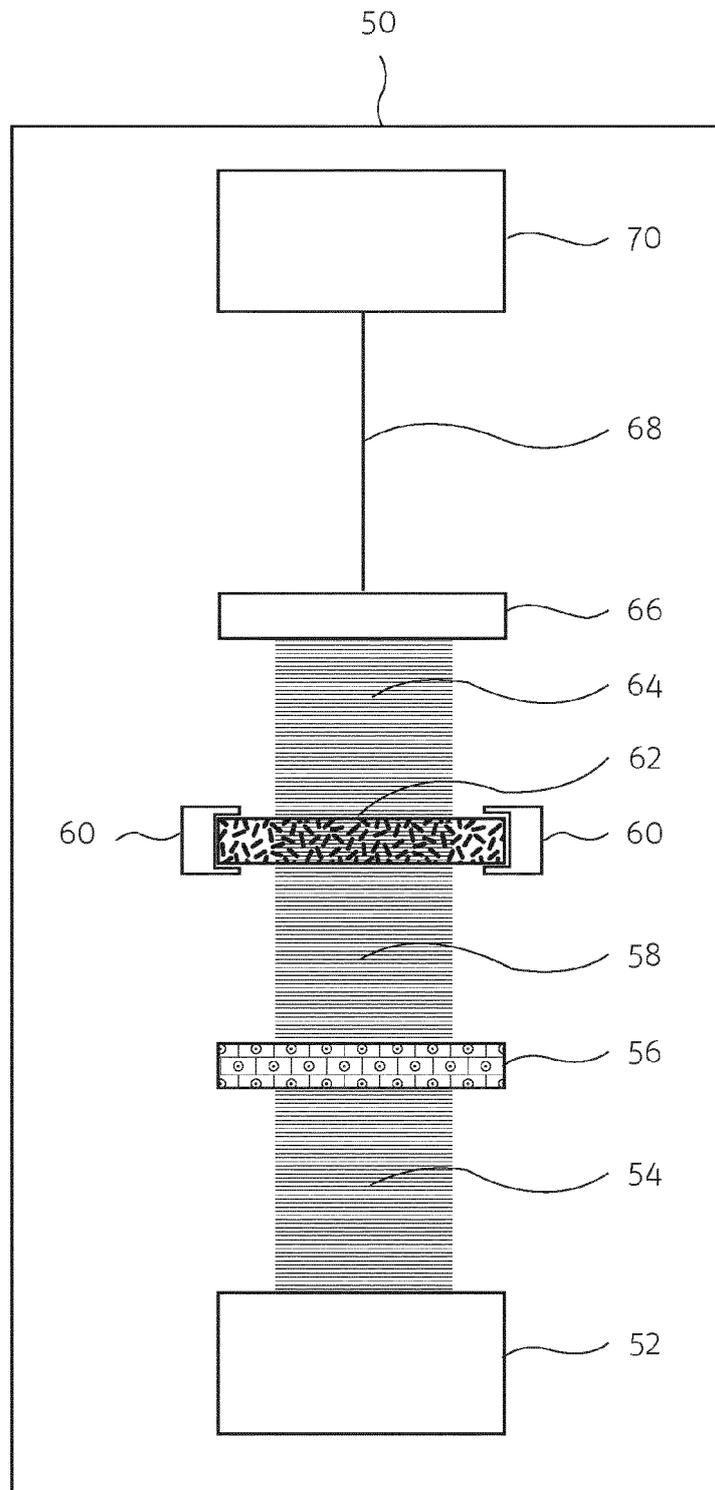


Fig. 3

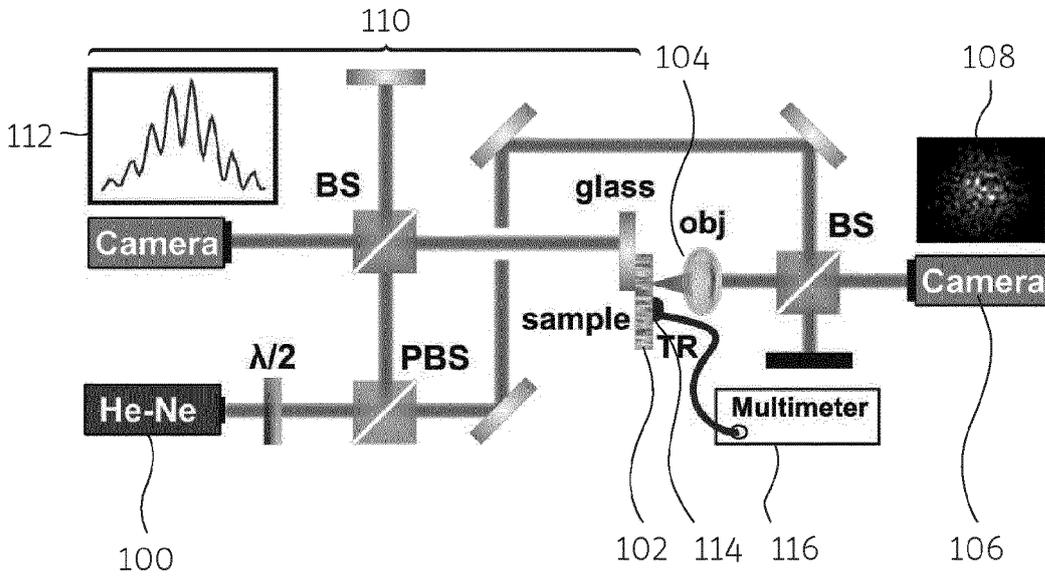


Fig. 4

(a)

(b)

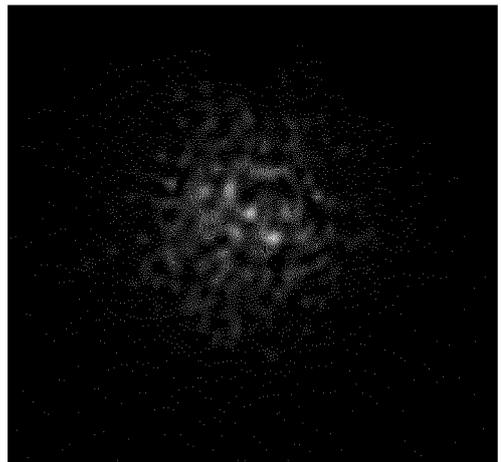
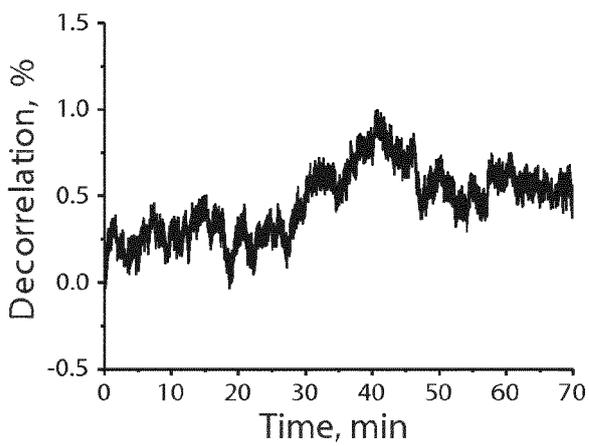


Fig. 5

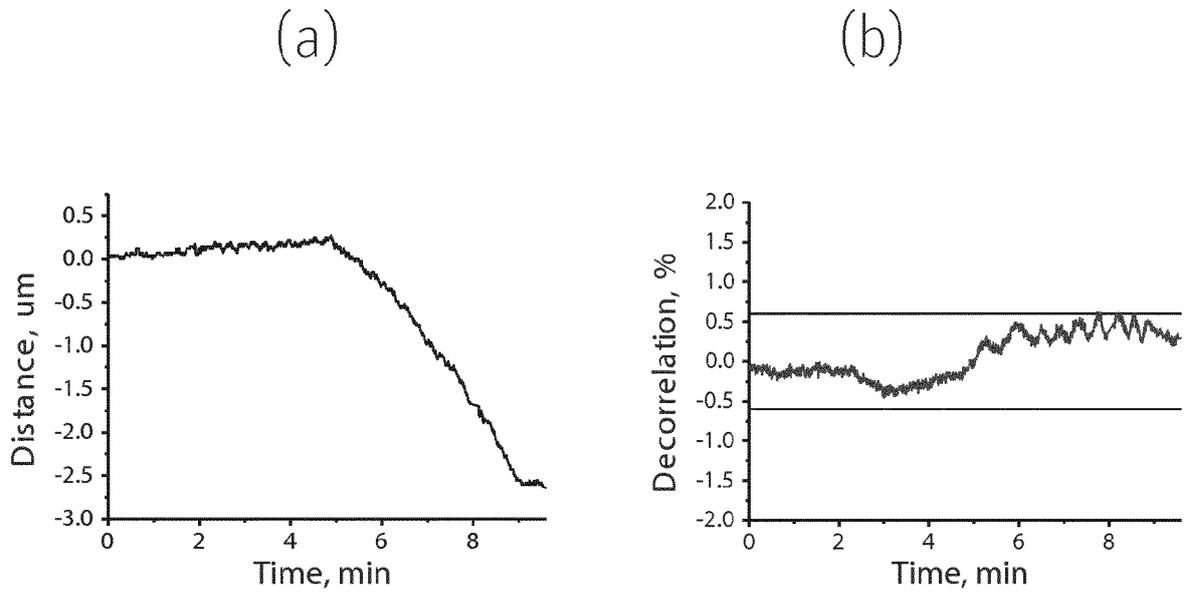


Fig. 6

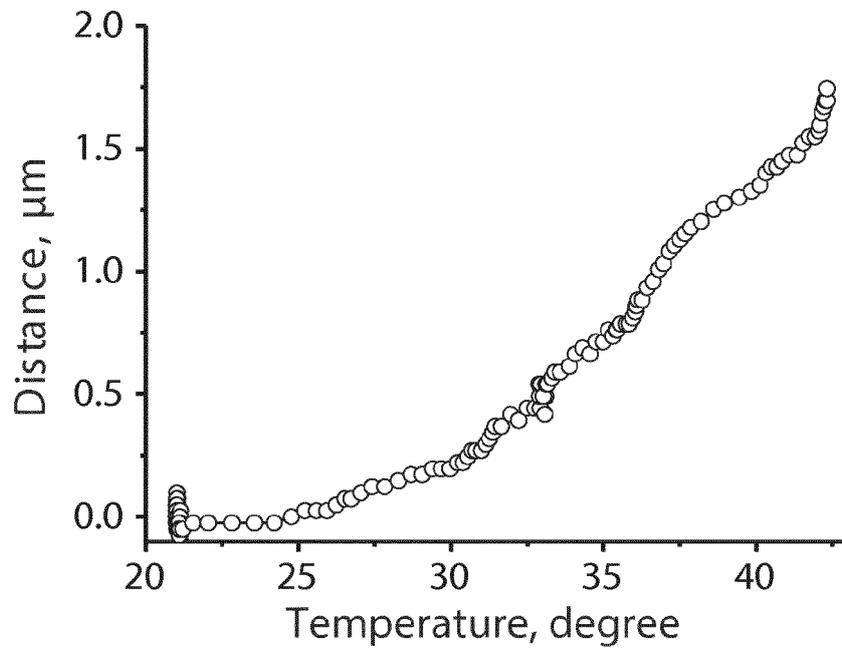


Fig. 7

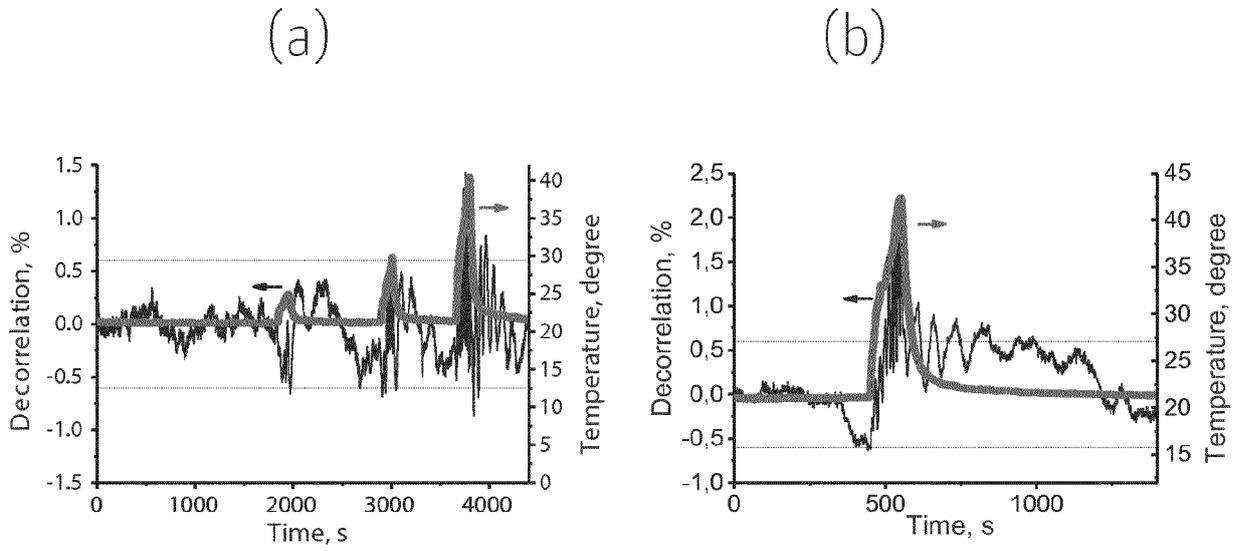


Fig. 8

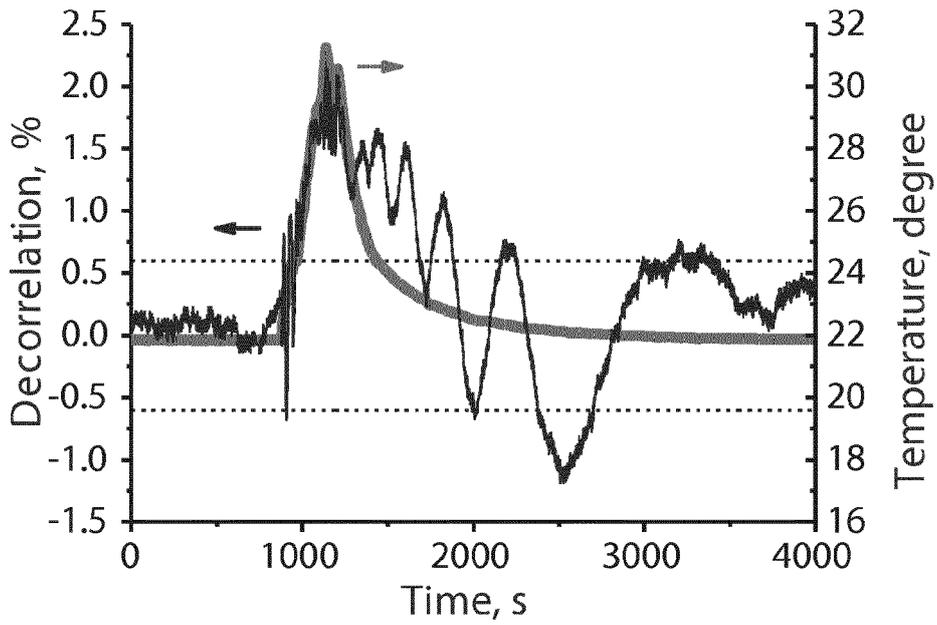
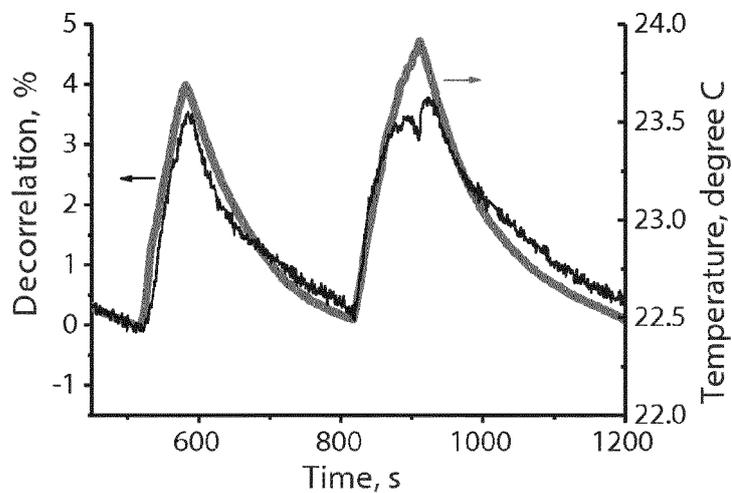
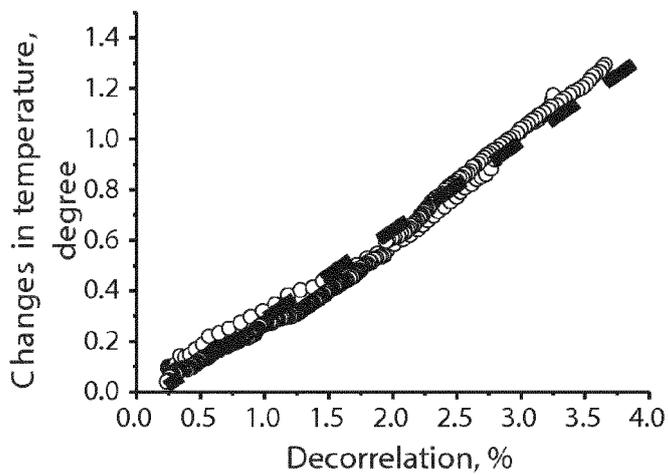


Fig. 9

(a)

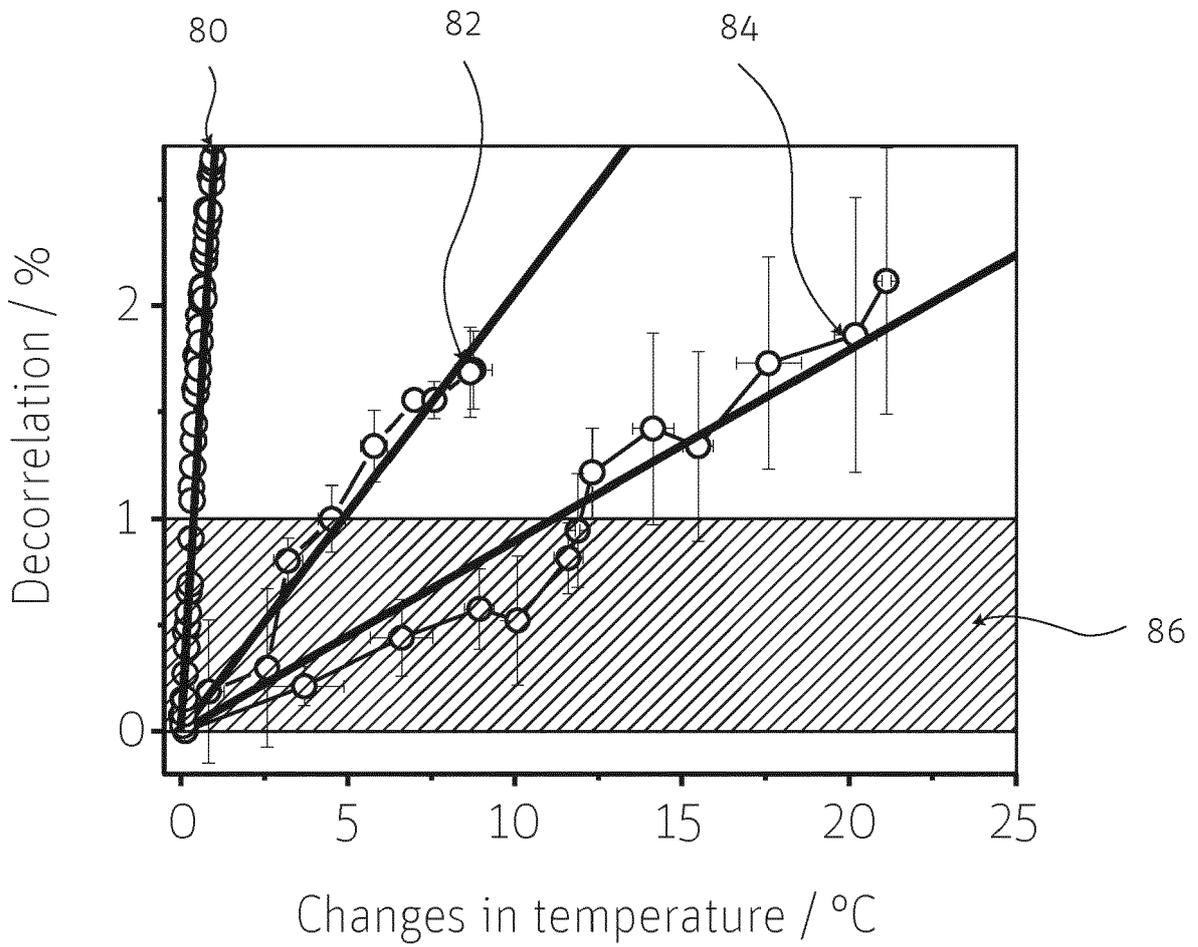


(b)



Equation	$y = A + B \cdot x$		
Adj. R-Squa	0.98397		
		Value	Standard Err
O1	A	22.3398	0.00374
O1	B	0.34893	0.00222

Fig. 10





EUROPEAN SEARCH REPORT

Application Number
EP 16 17 2091

5

10

15

20

25

30

35

40

45

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	Sebastianus A Goorden ET AL: "Quantum-Secure Authentication with a Classical Key", 1 March 2013 (2013-03-01), XP055168644, DOI: 10.1364/OPTICA.1.000421 Retrieved from the Internet: URL:http://arxiv.org/abs/1303.0142	1,3,9, 10, 12-15, 17-22	INV. G09C5/00 H04L9/08 H04L9/32
Y	* page 1 - page 3 *	2,4,5, 11,16	
Y	----- EP 2 230 794 A2 (UNIV MUENCHEN TECH [DE]; RUEHRMAIR ULRICH [DE]) 22 September 2010 (2010-09-22) * paragraph [0234] - paragraph [0241] * * figure 10 *	2,4,5, 11,16	
A,D	----- EP 2 693 685 A1 (UNIV TWENTE [NL]; UNIV EINDHOVEN TECH [NL]) 5 February 2014 (2014-02-05) * paragraph [0030] * * paragraph [0055] - paragraph [0063] * * figures 2,3 *	1-22	TECHNICAL FIELDS SEARCHED (IPC)
A	----- BORIS SKORIC ET AL: "Security of Quantum-Readout PUFs against quadrature based challenge estimation attacks", INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH,, vol. 20130304:202043, 4 March 2013 (2013-03-04), pages 1-11, XP061007355, [retrieved on 2013-03-04] * paragraph [01.3] *	1-3	G09C H04L
A,D	----- US 2013/243187 A1 (HORSTMAYER ROARKE [US] ET AL) 19 September 2013 (2013-09-19) * paragraph [0117] - paragraph [0145] *	1-22	
The present search report has been drawn up for all claims			
Place of search Munich		Date of completion of the search 10 November 2016	Examiner Bec, Thierry
CATEGORY OF CITED DOCUMENTS X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document			

1
EPO FORM 1503 03/02 (P04/C01)

50

55

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 16 17 2091

5 This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

10-11-2016

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 2230794 A2	22-09-2010	EP 2230794 A2 WO 2010105993 A2	22-09-2010 23-09-2010
EP 2693685 A1	05-02-2014	EP 2693685 A1 US 2015229482 A1 WO 2014019678 A1	05-02-2014 13-08-2015 06-02-2014
US 2013243187 A1	19-09-2013	NONE	

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- EP 2693685 A1 [0003]
- US 20130243187 A1 [0004] [0075]
- WO 2007046018 A1 [0005]
- US 20080121708 A1 [0006]

Non-patent literature cited in the description

- **J. BUCHANAN ; R. COWBURN ; A. JAUSOVEC ; D. PETIT ; P. SEEM ; G. XIONG ; D. K. FENTON ; D. ALLWOOD ; M. BRYAN.** Forgery: Fingerprinting documents and packaging. *Nature*, 2005, vol. 436, 475 [0007]
- **P. W. H. PINKSE.** Quantum-secure authentication of a physical unclonable function. *Optica*, 2014, vol. 1, 421 [0007]
- **A.P. MOSK ; A. LAGENDIJK ; G. LEROSEY ; M. FINK.** Controlling waves in space and time for imaging and focusing in complex media. *Nat. Photon.*, 2012, vol. 6, 283 [0007]
- **R. PAPPU ; B. RECHT ; J. TAYLOR ; N. GERSH-ENFELD.** Physical One-Way Functions. *Science*, 2002, vol. 297, 2026 [0007]
- **R. HORSTMAYER ; B. JUDKEWITZ ; I. M. VELLEKOOP ; S. ASSAWAWORRARIT ; C YANG.** Physical key-protected one-time pad. *Sci. Rep.*, 2013, vol. 3, 3543 [0007]