(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 February 2014 (06.02.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/019678 A1

(51) International Patent Classification:
H04L 9/32 (2006.01)

(21) International Application Number:
PCT/EP2013/002249

(22) International Filing Date:
30 July 2013 (30.07.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
EP12005527 30 July 2012 (30.07.2012) EP

(71) Applicants: **UNIVERSITEIT TWENTE** [NL/NL]; Drienerlolaan 5, NL-7522 NB Enschede (NL). **TECHNISCHE UNIVERSITEIT EINDHOVEN** [NL/NL]; Den Dolech 2, NL-5612 AZ Eindhoven (NL).

(72) Inventors: **PINKSE, Pepijn W.H.**; Wagnerlaan 10, NL-7522 KJ Enschede (NL). **MOSK, Allard, P.**; Ankrot 92, NL-7523 LE Enschede (NL). **ŠKORIĆ, Boris**; Vivaldistraat 29, NL-5216 EK 's Hertogenbosch (NL).

(74) Agent: **TESCH-BIEDERMANN, Carmen**; Athene Patent, Hanns-Schwindt-Str. 11, 81829 Munich (DE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

— *with amended claims (Art. 19(1))*

(54) Title: QUANTUM SECURE DEVICE, SYSTEM AND METHOD FOR VERIFYING CHALLENGE-RESPONSE PAIRS USING A PHYSICALLY UNCLONABLE FUNCTION (PUF)

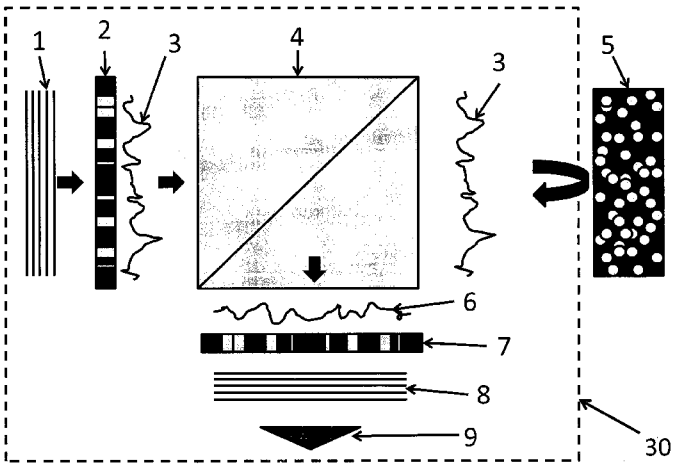


Fig. 3

(57) Abstract: The present invention provides a quantum secure device, system and method for verifying challenge-response pairs using a physically unclonable function (PUF). Exemplarily, a device for verifying challenge-response pairs comprises: a wave source, in particular a light source; a challenge creating means for creating a challenge, in particular an optical challenge, to be sent to a PUF, in particular when receiving signals from the wave source; a response transformation means for verifying a response, in particular an optical response, from a PUF; and a detector for reading out the result of the verification carried out by the response transformation means. Preferably, the number of interaction particles, in particular photons, in the challenge is less than the number of parameters needed to fully describe the setting of the challenge creating means which guarantees quantum security. According to a preferred embodiment, the challenge creating means and/or the response transformation means are/is adapted to carry out wavefront shaping on provided light.

WO 2014/019678 A1

Quantum secure device, system and method for verifying challenge-response pairs using a physically unclonable function (PUF)

Field of the invention

The invention is related to the field of physically unclonable functions (PUFs), in particular to the field of optical PUFs. More particularly, it is related to a quantum secure device, system and method for verifying challenge-response pairs (CRPs) using a PUF. Amongst other purposes, the invention is suitable for use with credit cards and other authentication cards, allowing access to a secret or resource.

Background art

Secure communication and authorization is a highly important topic these days. Many secure communication and authorization schemes rely on cryptographic systems and methods. In classical cryptography, the mathematically (still not entirely proven) fact is used that some mathematical functions can be calculated in one direction without any problems, but solving the inverse mathematical problem is hardly possible; at least this would require extremely high and time-consuming computational efforts. However, these computational efforts will suddenly be significantly reduced when the first quantum computers will start operation. Therefore, one is looking for other approaches being inherently secure. One approach is quantum cryptography. Basically, this is a physical approach relying on the fact that each measurement influences unknown quantum states, and it is therefore in principle possible to find out about an eavesdropper. However, quantum states are rather fragile states, and until today it is rather hard to prepare and handle them appropriately, in particular over larger distances.

In practical cryptography, a physically unclonable function or PUF [1,2] is a function that is embodied in a physical structure and is easy to evaluate, but hard to predict and assumed to be physically unclonable because of a strong dependence on uncontrollable aspects of the manufacturing process. PUFs have a unique challenge-response behaviour. For these reasons they are of interest as means of authentication.

Typically, a PUF owner should prove access to a secret by presenting his PUF to a verifying party. The verifying party sends a signal called challenge to the PUF, and the PUF then creates a unique and hard to predict reply signal called response. This response is supplied back to the verifying party such that it can be verified that the PUF owner actually has authorized access to the secret or resource.

By now many PUF-like systems have appeared in the literature: optical PUFs [1, 2], delays in integrated circuits [3], dielectric properties of security coatings [4], two-dimensional fiber-optic configurations [5], radiofrequent probing of wire configurations [6] and thin-film resonators [7], laser probing of fibers in paper [8], startup values of SRAM cells [9], butterfly PUFs [10], phosphor patterns [11], phase-change memory states [12].

Several patent applications directed to PUFs exist as well: WO 2007/046018 A1 is directed to an optical PUF with a combined sensor and display. It applies light which is scattered by a light scattering element comprising a transmissive material which contains randomly distributed light scattering particles which scatter incident light such that a random speckle pattern is created and spread over light detecting elements. The key idea of the cited reference is to include reflecting picture elements into the device in such a manner that it becomes possible to modify applied challenges by activating and switching off the picture elements, thereby also modifying the corresponding response/ speckle pattern.

US 2006/0095773 A1 is directed to an authentication system, a light emitting device, authentication device and an authentication method which applies an emission-angle dependent light emitting device and a corresponding emission-angle dependent light detector.

WO 2005/059629 A1 is directed to an optical method and apparatus for detection of a speckle based PUF and focuses on the definition of criteria employed to determine the size of pixels of a detector that will give rise to detection of all relevant bits (i.e. the pixels are small enough) without too much redundancy (i.e. the pixels are large enough).

US 2008/0121708 A1 is directed to physical credentials and related methods. Directional albedo of an article is measured and stored. When the article is later presented, it can be confirmed to be the same particular article by re-measuring the albedo function, and checking for correspondence against earlier stored data. The disclosed device and method

gains its security from statistics considerations. However, the disclosed device and method is not inherently secure, in particular not quantum secure.

US 2007/046018 A1 is directed to an integrated physical unclonable function (PUF) with combined sensor and display. A specific creation of challenge response pairs is disclosed. However, quantum security is not achieved.

WO 98/28707 is directed to a method and an apparatus for enhancing the integrity of visual authentication. The illumination of an object is modulated for hindering attacks by replaying recorded images. The object is no PUF. Quantum security is no topic.

In all existing PUFs, the security of the verification relies on the fact that the validator knows he is probing the properties of a physical entity such as an integrated circuit, a SRAM cell, a phosphor layer, etc. In case the PUF owner doesn't trust the validator, he doesn't want to give away his PUF for checking. Consequently, the best a validator can do is to try to check from a (possibly small) distance, in which case he can be fooled by an intelligent attacker system emulating the PUF. Highly desired for authentication processes is a secure and practical authentication protocol which does not rely on a trusted remote reader device or on examining the PUF to make sure it is a physical object of the expected size, weight and complexity.

A possible direction was recently given by B. Škorić in a mathematical abstract paper [13], who suggested a quantum secure readout of a classical PUF that is challenged using a quantum state, and who's response is also a quantum state. The protocol allows for authenticating a QR-PUF remotely without reliance on a trusted remote reader device. The paper by B. Škorić did not suggest a physical implementation and suffers from the fact that its security proof uses (necessarily fragile) quantum states as key element.

Description of the invention

It is therefore the objective technical problem to be solved to provide a secure device, system and method for authentication purposes which can overcome the above mentioned disadvantages. In particular, it is aimed to provide a secure device, system and method of the aforementioned type that is based on PUFs. Even more particular, the device, system and method shall guarantee security even in cases in which the properties of the PUF are publicly known and might be emulated.

The object is solved by the subject matter defined in the independent claims. Dependent claims are directed to advantageous embodiments.

According to a first aspect of the invention, the invention is directed to a device for verifying challenge-response pairs, comprising:
- a wave source, in particular a light source;
- a challenge creating means for creating a challenge, in particular an optical challenge, to be sent to a PUF, in particular when receiving waves emitted from the wave source;
- a response transformation means for verifying a response from a PUF; and
- a detector for reading out the result of the verification carried out by the response transformation means.

The invention directed to the device for verifying challenge-response pairs presumes that challenge-response pairs have been previously defined (an example for such a definition of challenge-response pairs will be further addressed below). The claimed device is applicable for verifying challenge-response pairs, in other words to make sure that a challenge-response pair is valid.

The device for verifying challenge-response pairs comprises a wave source, in particular a light source. In general, there exist several different types of wave sources that can in principle be used in the present invention. The important aspect here is that the wave source emits waves that also have particle character (wave-particle-dualism). The invention uses both the wave characteristics as well as the particle characteristics in its realization. Furthermore, when assuming that the PUF interaction shall include a scattering process, such wave types are suited that allow for such a unique scattering interaction in the PUF. As already mentioned above, an important type of a wave source according to the invention is therefore a light source. However, there exist several other examples of suited wave sources: sound waves, in particular ultra sound waves, plasmons, plasmon-polaritons, electrons, holes, or even ions or elementary particles.

In a preferred embodiment, the wave source is a coherent light source. Here, the term "coherent light" means light with a narrow enough bandwidth to create a high-contrast-speckle pattern, and not "coherent" in the quantum optical sense where it is also used to describe the statistics. Preferably, the coherent light source is a laser. Preferably, the light source can be operated to emit weak light. In a preferred embodiment, the coherent light source is a laser adapted to emit pulses of only a limited number of photons. It is not

necessarily the case that just one photon is emitted in one laser pulse, however, this is also a possible embodiment. According to a preferred embodiment, one laser pulse comprises approximately up to 250 photons. In a preferred embodiment, a laser diode is applied as the coherent light source. Other laser types can also be used. In principle, there exist no limitations for the applied laser frequencies; however, it makes sense to choose laser frequencies that allow for a good interaction with a selected optical PUF. Preferably, the applied frequency/frequencies is in the visible-infrared part of the spectrum.

The device for verifying challenge-response pairs comprises a challenge creating means for creating a challenge, in particular when receiving waves from a wave source. In most cases the wave source and the challenge creating means are provided as separate means. Still, these means can be combined or integrated with one another. In a further embodiment it is even possible that the wave source as such also acts as the challenge creating means. In the letter case the challenge creating means does not (separately) receive waves from the wave source. The challenge has to be sent to a PUF means for interacting with the challenge, thereby creating a response to the challenge. In this manner, a challenge presented to the PUF will lead to a respective response from the PUF, thereby generating a unique challenge-response pair. In the known systems for verifying challenge-response pairs, there is provided a detector for directly or indirectly reading out the thus created response from the PUF. In other words, the response is in principle analyzed in detail, and the response can be fully characterized due to this analysis. Then, a comparison of the actual response generated from the PUF is compared to the response theoretically expected when presenting a known challenge to the PUF. If the actual response fits to the expected theoretical response, the challenge-response pair is verified, and for example access to a secret or resource is allowed.

However, according to the present invention, the response from the PUF is not fully characterized with the response transformation means, there is no direct or indirect readout and no full description of the response because of a measurement of the response signal itself. In contrast thereto, the present invention applies a response transformation means for verifying the response from the PUF which is no readout and which does not necessarily allow for a full description of the response generated by the PUF. The response transformation means preferably acts on the response signal in the manner of a transformation or conversion, preferably in the manner of a reversion or inversion or projection. It transforms or converts the response signal such that a detection for reading out the result of the verification becomes possible. It is noted that a detection reading out the result of the verification is generally not possible without prior application of the response

transformation means. This becomes a key aspect when talking about quantum security (see below).

The response transformation means is suited for verifying the response, and this implies that its specific configuration has to be set in accordance with a known/preselected challenge. The response transformation means is therefore no means that interacts in a completely identical manner with all possibly presented signals/ responses, but its setting has to be chosen depending on the applied challenge sent out by the challenge creating means. The response transformation means can then act on the presented response signal in a challenge-response-pair specific manner that leads to an output from the response transformation means. This output can then be detected (or possibly in fact not detected) in order to judge whether a challenge-response pair was valid or not. If it was valid, then the correct PUF had been presented to the device for verifying challenge-response pairs.

According to a preferred embodiment of the invention, the action of the response transformation means is of the type of a reversion or inversion or projection and basically reverses or inverts or projects a response signal. The effect of the inversion or reversion or projection is that, after the reversion or inversion or projection, readout of the result of the verification procedure becomes possible. A reversion or inversion acting on the response signal brings the signal back into an original condition – it is however normally not the case that the signal outputted by the response transformation means is identical to an original state that was previously sent to the challenge creating means. A projection can project a response onto a state that is well suited for later measurement. The original condition re-established or the characteristics of the state resulting from the projection by action the response transformation means can for example be a common phase of the wavefront in all channels, common amplitude or common polarization, etc. These common characteristics can be requirements that have to be fulfilled for successfully carrying out a later measurement / detection – in particular with respect to a signal strength needed when only a few interaction particles are used for verification in order to guarantee quantum security.

According to a preferred embodiment of the invention, the nature of the response transformation means is of the same type as that of the challenge creating means. This means that the physical interactions carried out using the challenge creating means on the one hand and the response transformation means on the other hand are basically the same; however, it is not required that the detailed interaction is identical in all aspects.

According to a preferred embodiment of the invention, the challenge creating means and/or the response transformation means are/is adapted to carry out wavefront shaping on provided light. Wavefront shaping is a technique that was recently developed by one of the inventors [14, 15], but until today it has never been applied in connection with challenge-response pairs and PUFs. According to wavefront shaping techniques, it was for example demonstrated to focus coherent light through disordered scattering media by the construction of wavefronts that invert diffusion of light. More concretely, wavefront shaping allows for the construction of input wavefronts that exactly compensate the phase delays of paths through the randomly scattering medium such that the light leaving the medium constructively interferes on one spot, forming a focus. A concrete example for a challenge creating means and/or a response transformation means are spatial light modulators (SLMs) for manipulating the phase and/or amplitude of light. According to a preferred embodiment of the invention, two regions of the same SLM can be used to embody the challenge creating means and the response transformation means, respectively.

According to the claimed device for verifying challenge-response pairs, the challenge creating means as well as the response transformation means act on a provided wave/ waves, in particular light, in a manner depending on the properties and definition of the challenge-response pair having been chosen for verification purposes. Then, the claimed device comprises a detector for reading out the result of the verification carried out by the response verification means. Once again, it shall be stressed that this readout is no readout of the response signal itself, but it is a detection of the signal generated by the response transformation means. Therefore, the device for verifying challenge-response pairs according to the invention provides for the first time an indirect readout of the response generated by the applied PUF, wherein it is not necessary to fully characterize the response. This can significantly facilitate systems for verifying challenge-response pairs.

Furthermore and most important, the above described device for verifying challenge-response pairs offers a possibility to implement a quantum secure device for verifying challenge-response pairs: Advantageously, the number of interaction particles, in particular photons, in the challenge is less than the number of parameters needed to fully describe the setting of the challenge creating means. In each case, a challenge-response pair can be described mathematically in a Hilbert space of appropriate size. A very simplified and comprehensive explanation of this quantum security is as follows: Assume that an eavesdropper wants to copy a challenge (or response) signal. Then, ideally, he has to find out about *all* characteristics/ settings of the challenge (description in Hilbert space of appropriate size). This has to be done by a *measurement*. However, in order to classically

determine *one* characteristics or setting of the challenge, at least *one* interaction particle has to be measured. The measurement of just *one* interaction particle can deliver the information about just *one* characteristic or setting. But – due to the wave nature of the interaction particle – it is possible to code *more than one* characteristics or settings in the quantum mechanical state of *just one* interaction particle. However, it is absolutely impossible to completely read-out or reconstruct *all* characteristics or settings from measuring *just one* interaction particle. One might say that the quantum mechanical extent of information carried by an interaction particle can be much higher than the classical extent of information that can be extracted from the interaction particle by a measurement. The above described quantum security can be achieved independently from the concrete physical nature/ definition of the challenge response pair and the concrete physical nature of the interaction particles. The fascinating device-inherent quantum security is a very general finding.

According to a preferred embodiment of the invention, the challenge or/and a response is/are defined by a physical property of photons, in particular phase information, amplitude information, polarization information, frequency information, spatial information and/or time information of photon(s). Preferably, the challenge or/and response is described by a spatial distribution, in particular a two-dimensional distribution, of a physical property of photons, a frequency distribution of a physical property of photons and/or a time distribution of a physical property of photons. The physical property or properties can be selected from the properties listed above. In a suited Hilbert space, the description of the challenge-response pair is complete in that sense that all parameters for defining the challenge and the response are known/can be set. Giving a more illustrative example, the different channels in a spatial light modulator can be used to characterize a challenge by defining the setting for the challenge creating means. If, however, a coherent light pulse is provided to the challenge creating means, which contains less photons than the number of parameters needed to fully describe the setting of the challenge creating means (for example the number of channels in a spatial light modulator), then it becomes physically impossible that an eavesdropper reads out the challenge completely, looks up a respective response and sends the response back to the response transformation means. The full description of the wavefront needs more information than contained in a measurement of the few photon pulse. In other words, the number of photons (or more generally: interaction particles) is just too small for completely characterizing the challenge and thus copying the challenge for emulation purposes.

Though the security of the described device for verifying challenge-response pairs relies on the rules of quantum mechanics (more precisely on the extent of quantum mechanical information), the device itself does not suffer from the principle problem of fragile quantum

mechanical states. Of course, the claimed device could in principle also work with just one photon emitted from a the light source and sent to the challenge creating means and so on. A photon can also be temporally shaped. However, using just one single photon is not necessary in order to guarantee quantum security. Preferably, more than photon is used. A typical number of photons in the optical challenge can be approximately 250 photons, in combination with for example 1000 channels in the challenge creating means.

As already mentioned above, a challenge-response pair according to the invention can be described by a spatial distribution, in particular a two-dimensional distribution, of a physical property of photons. Alternatively, a challenge-response pair according to the invention can be described by a time distribution or frequency distribution of a physical property of photons. Once again such a physical property of a photon can then be phase information, amplitude information, polarization information, frequency information, time or spatial information.

The principle of the present invention is broadly applicable to devices for verifying challenge-response pairs. Furthermore, it has to be noted that wavefront shaping techniques have been applied for devices for verifying challenge-response pairs for the first time.

According to a preferred embodiment of the invention, a focusing means is provided for focusing waves, in particular light, onto the detector for detection. Preferably, the focusing means is provided between the response transformation means and the detector. The focusing means can for example be a focusing lens. Alternatively, the response transformation means can be adapted to also act as the focusing means, and then no additional focusing means for focusing waves onto the detector is needed. When for example wavefront shaping techniques are applied, in particular in the response transformation means, the focusing means allows for focusing even extremely weak light pulses to a focusing point, since the response transformation means can act on the response in such a manner that the phases of all photons coincide which is a prerequisite for focusing. The problem is even more severe, since photon losses during PUF interaction inevitably will occur. Focusing in principle allows for detection applying optical detection methods well established in the art.

According to a preferred embodiment, the spatial detection range of the detector is point-like or/and the detector is adapted to carry out single photon counting. Preferably, these features are combined with the provision of a focusing means as mentioned above. The sole thing that is detected by a detector which is point-like is the number of photons or light energy. The detector then does not gain any information about a spatial distribution of photons arriving at

the detector. According to a preferred embodiment, the detector is an avalanche photo diode (APD). Of course, it is in principle also possible to apply a detector which is not point-like, such as for example a charge-coupled device (CCD).

According to a preferred embodiment of the invention, the device for verifying challenge-response pairs is adapted such that a positive result for verification is distinguished from a negative result for verification based on a preselected number of photons detected/detectable in the detector for one challenge-response pair. It is for example possible to define a threshold number of photons (or more general: interaction particles), the detection of which indicating that the challenge-response pair was valid. This is possible because the number of photons (interaction particles) arriving at the detector can be estimated in advance, and in general the Poisson distribution of photons (interaction particles) arriving at the detector is known.

According to a second aspect of the invention, the invention is directed to a system comprising the device for verifying challenge-response pairs as described in detail above and a PUF means. The PUF means interacts with the challenge, thereby creating a response to the optical challenge.

Preferably, the PUF means is an optical PUF. The PUF means can be realized in different manners. The PUF means can in particular act on the basis of light scattering, either in transmission or in reflection operation mode. The PUF means can for example be a pigment such as ZnO or TiO_2 provided on glass, or more stably in glass ceramics (glass containing nanoparticles) or in PMMA (like a DVD), or ceramics themselves. Another example is biologic material which has the potential to authenticate people by the unique properties of their body. Such unique biometric data can for example be teeth, bones or even parts of the human eye. These materials fulfill a general requirement for PUF interaction, namely that the material of the PUF/ the scattering media included in the PUF have a scattering mean-free path which is short and well controlled. A rough surface alone cannot be used as a PUF.

According to a third aspect of the invention, the invention concerns a method for verifying challenge-response pairs. This method comprises the following steps:
- emitting a wave, in particular light;
- creating a challenge, in particular an optical challenge, in particular by directing the emitted wave onto a challenge creating means;
- sending the challenge to a PUF means, thereby creating a response, in particular an optical response, to the challenge;

- verifying the response by directing the response onto a response transformation means,;
- reading out the result of verification carried out by the response transformation means with a detector.

The method for verifying challenge-response pairs corresponds to the above described device and system for verifying challenge-response pairs. In particular, the method for verifying challenge-response pairs can be executed applying the system for verifying challenge-response pairs as described in detail above. The wording applied in the claimed method for verifying challenge-response pairs also corresponds to the wording used for describing the system for verifying challenge-response pairs. The interpretation and specific embodiments described by the respective wording are therefore also identical.

Similar to the system for verifying challenge-response pairs, the method for verifying challenge-response pairs differs from the known prior art in the step of verifying the response by directing the response onto a response transformation means, and further in the step of reading out the result of verification carried out by the response verification means – not the response itself – with a detector.

The above described method once again allows for quantum secure verification of challenge-response pairs: According to an advantageous embodiment, the number of interaction particles, in particular photons, in the challenge is smaller than the number of parameters needed to fully describe the setting of the challenge creating means. So once again the full description of the wavefront needs more information than contained in a measurement of a single pulse of interaction particles. It is therefore impossible for an eavesdropper to read out the challenge in order to emulate a PUF. The presence of a real physical entity can therefore be securely distinguished from an emulation of the PUF.

According to a preferable embodiment, the step of reading out the verification result comprises the step of interaction particle counting, in particular photon counting. In particular, it is possible to define a threshold number of interaction particles, in particular photons, that – when detected – will be regarded as a positive verification result.

According to the invention, it is also possible that some or all of the above mentioned method steps are carried out repeatedly. A repetition of method steps may quickly enhance security of the claimed method even more due to grounds of statistics. The sequence of repeated verifications may include spoof challenges –response pairs that should, for the correct PUF,

produce a negative verification result, thereby foiling attacks that always produce a positive result by sending signals of any kind to bypass the verification device.

As already mentioned above, the device, system and method for verifying challenge-response pairs presumes a predefinition of these pairs. In principle, the person skilled in the art will understand from the basic ideas of the invention how such a predefinition can be carried out. However, in the following, an explicit example will be given which is in particular well suited for use with optical PUFs.

The example device for defining challenge-response pairs is based on an interferometric setup, the device comprising:
- a wave source, in particular light source;
- a detector adapted to detect a speckle pattern;
- wherein the device is configured such that waves from the light source can reach the detector along two different paths, thereby realizing an interferometric setup;
- the first path comprising the following elements:
    - a challenge creating means for creating a challenge, in particular an optical challenge, to be sent to a PUF, in particular when receiving signals emitted from the wave source;
    - a response transformation means for verifying a response from a PUF ; and
- one of the paths, in particular the second path, comprising means to vary its path length.

The above device for defining challenge-response pairs partly comprises elements of the above described device for verifying challenge-response pairs. In particular, the elements of the first path (challenge creating means and response transformation means) are identical. However, in the device for defining challenge-response pairs, at least one of the paths, in particular the second path, comprises means to vary its path length, and therefore an interferometric setup is realized. Dividing waves, in particular light, into two parts can be realized with known techniques, for example by using beam splitters. The interferometric setup allows for example for the definition of challenge response pairs based on phase information, for example phase information about a shaped light front. The phase setting for the response transformation means can be determined for a pre-selected challenge. However, it has to be noted that a phase-shifting interferometric setup is not the only possibility to determine necessary phase information.

The wave source is a rather strong wave source – contrary to the wave source advantageously applied in the device for verifying challenge-response pairs. However, the

physical device embodying the wave source can still be identical: when applied in the system for defining challenge-response pairs, high or full power of the wave source can be applied; on the other hand, when using the wave source in the device for verifying challenge-response pairs, the wave source can be dimmed and chopped.

The detector of the system for defining challenge-response pairs is adapted to detect a speckle pattern. In other words, the detector allows for a two-dimensional resolution of the detected signals. This requirement is for example fulfilled by a CCD.

According to the example, the challenge creating means and the response transformation means can be SLMs for manipulating the phase and/or amplitude of light.

Furthermore, the device for defining challenge-response pairs comprises a phase calculating means adapted to calculate the phase of all detectable or detected speckles. This phase calculating means can for example comprise a software routine implemented in a computer.

A system for defining challenge-response pairs can be operated by the following method:
A method for defining challenge-response pairs using the system for defining challenge-response pairs based on an interferometric setup, wherein the challenge creating means and the response transformation means are adapted to manipulate the phase of incident waves, comprising the following steps:
- choosing a configuration for the challenge creating means, thereby setting a challenge;
- setting the response transformation means to zero;
- emitting signals from the wave source to the interferometric setup;
- varying the path length of one of the paths, in particular that of the second path;
- detecting speckle patterns for each of the varied path lengths;
- calculating the phase of the wavefront emitted from the PUF based on the measurement results for the speckle patterns;
- setting the configuration of the response transformation means such that its action on the response emitted from the PUF is that of a conjugate phase.

Setting the response transformation means to zero as mentioned above means that the response transformation means does not actively manipulate the phase of light incident to the response transformation means. However, it is of course possible that a phase shift that is equal in all channels of the response transformation means can occur.

The steps of detecting a speckle pattern and varying the path length of one of the paths, in particular that of the second path, are repeated several times. Preferably, the path length of

the second path is varied for pi in several, quasi continuous steps, for example in 50 steps. However, there also exist techniques which do not require the repetition of steps in order to vary path lengths in order to find out about the phase. Instead, there also exist one-shot techniques, according to which several phase constellations are simultaneously detected, allowing for a calculation of the respective phase to be set in the response transformation means.

As mentioned above, the configuration of the response transformation means is set in such a manner that its action on the response/ wavefront emitted from the PUF is that of a conjugate phase. In other words, the response transformation means has the effect to bring the phase of the light scattered from the PUF back into phase. It is noted that the conjugate phase to which action the response transformation means is set is of course not the conjugate phase to the setting of the challenge creating means.

As a further example, the method for defining challenge-response pairs can further comprise a verification step indicating that the determined setting of the response transformation means (7) is correct.

Exemplarily, this verification step can comprise the following steps:
- blocking the second path;
- replacing the detector adapted to detect a speckle pattern with a point-like detector or/ and a detector adapted to carry out single interaction particle (photon) counting;
- dimming the wave source;
- focusing the wave exiting from the first path; and
- detecting the focused wave.

It goes without saying that the basic method steps as well as the additional method steps can be carried out repeatedly for different settings of the challenge creating means, thereby defining a plurality of challenge-response pairs.

Exemplarily, the method for defining challenge-response pairs can further comprise the following step:

- calculating a threshold number of interaction particles, in particular photons, that shall be at least detected with the chosen experimental setup when a valid challenge-response pair is used in combination with a correct PUF.

This kind of calculation is based on pure statistics and the threshold number can be calculated without any problems when the relevant method steps are repeated sufficiently

often in order to fulfill statistics requirements. In this connection, it is also possible to estimate the values of false positive and false negative responses detecting the focused light.

The present invention will be more fully understood by referring to the accompanying drawings, wherein:

Fig. 1: is a flowchart of CRP verification according to the state of the art;

Fig. 2: is a flowchart illustrating CRP verification according to the present invention in a schematic manner;

Fig. 3: shows a schematic setup for PUF verification according to a first embodiment of the present invention;

Fig. 4: shows a schematic experimental setup for defining valid CRPs;

Fig. 5: exemplarily shows detection results gained with an APD for a) a correct challenge-response pair (correct PUF) and b) a wrong challenge-response pair (wrong PUF); and.

Fig. 6: exemplarily illustrates a setting for challenge and shows detection results in form of an intensity distribution of light for a) a correct PUF and b) a wrong PUF.

Fig. 1 illustrates a CRP verification according to the state of the art in form of a flowchart. It shall depict principle method steps in CRP verification procedures. At the beginning, in method step S1, a database with CRPs is provided. The CRPs of the database have been previously defined; they have for example been measured using an appropriate experimental setup. According to method step S2, a challenge C out of the CRP database is chosen. The challenge is sent in step S3 to the PUF. According to step S4, the PUF answers with a specific PUF-response, and in step S5, the response from the PUF is read out. Then, in method step S6, it is judged whether the PUF response is identical with the theoretic response found in the database for the chosen challenge. If the CRP is correct, then in step S7 access to a secret is given. Otherwise, in step S8, the access procedure to the secret is stopped and the procedure ends.

Fig. 2 depicts a flowchart showing a CRP verification process according to the present invention. In order to stress the differences to the known CRP verification procedure depicted in Fig. 1, a box 40 highlights the differences of the present invention. Method steps S1 to S4 until the PUF response are in principle identical to the steps of the known CRP verification procedures. However, then, a response provided by the PUF is not read out directly or

indirectly, and the PUF response is not characterized (no measurement). Instead, in method step S5a, a response transformation procedure for verification is carried out. In step S5b, the result of this response transformation procedure is read out. In step S6a, it is judged whether the verification result was positive. If this is the case, then, in step S7, access to the secret is allowed. If the verification result was not positive, the access to the secret is stopped and the procedure ends. The replacement of response readout by a response transformation procedure for verification and readout of the result of this transformation procedure allows in principle for a quantum secure verification of challenge response pairs. With the help of the response transformation procedure for verification and respective readout of the transformation procedure result, it becomes possible to use quantum mechanical information included in the CRP for verification purposes, wherein the extent of quantum mechanical information is larger than any classical information that can be gained by a measurement process of the respective challenge or response.

In the following, we will more concretely concentrate on optical challenge response pairs interacting with an optical PUF. However, the skilled person will easily understand that the general principles of the optics realization can be easily transferred to other kinds of realization.

Fig. 3 shows a schematic setup for PUF verification. The system depicted in Fig. 3 comprises two main parts, the verifier 30 on the one hand and the key or PUF 5 on the other hand. The PUF 5 is presented to the verifier 30 in order to get access to a secret. It can for example be included in a credit card or in other cards applied in authorization and/or authentication procedures.

The verifier 30 is built up as follows: A coherent light source (not shown) emits laser pulses 1 having a flat wavefront in the depicted example. The laser pulse is comparatively weak and can for example comprise about 250 photons. The laser pulse 1 with the flat wavefront is sent to the challenge creating means 2 which is in the present case embodied by an SLM. The SLM 2 acts on the phase of the flat wavefront and shapes the wavefront into a random wavefront. Preferably, the setting of each channel in the SLM 2 is either zero or pi. Of course, a specific setting of the SLM 2 always results in the same shaped wavefront. The pulse with the random wavefront represents the challenge. In the present example, the SLM 2 has 1000 channels. These 1000 channels are provided in a grid-like manner, and the action of each channel can be individually set. The challenge 3 having passed the SLM 2 carries all information about the setting of the SLM 2, however, it is impossible to read out all of this information when detecting the challenge 3, because the challenge 3 just comprises

250 photons in the selected example, which is significantly less than the 1000 parameters needed to fully describe the setting of the SLM 2. It has to be born in mind that with the present experimental setup quantum effects play an important role. In particular, preparing a challenge just comprising *one* photon carrying the quantum mechanical information about *all* 1000 channels of the SLM 2 in principle is possible. However, it is preferred that the challenge contains more than one photon in average in order to have at least one detector click in case of a good CRP.

The number of channels in the SLM 2 is related to the number of controlled channels (K) in the PUF. In the present case, K is roughly the number of speckles, and the number of pixels in the challenge-forming SLM 2 must be chosen at least as high as K. In this context, a quantum security parameter S=K/n can be defined, wherein n denotes the number of photons in the challenge (or more general: the number of interaction particles). This parameter is preferably in the range $1 < S \leq K$.

The challenge 3 passes through a beam splitter 4 and is incident on the PUF 5 where it is scattered back to the beam splitter 4. It is noted that a PUF 5 can of course also work in a transmission mode, not just in a reflection mode. The wavefront that is scattered back from the PUF 5 represents the response 6. For ease of depiction, the response 6 is just depicted after having passed the beam splitter 4, but of course it is also present between the PUF 5 and the beam splitter 4. The wavefront of response 6 is specially shaped due to the interaction with the PUF 5. The response 6 is then sent to the SLM 7 which acts as the response transformation means. The setting of the SLM 7 has been chosen based on the knowledge about the setting of SLM 2; in particular, these two settings are normally neither identical, nor is the setting of the response transformation means 7 the conjugate setting to that of SLM 2. Instead, the setting of SLM 7 is such that it conjugates the phase of response 6. Having passed SLM 7, the wavefront of the pulse 8 has been shaped such that the phases in the pulse coincide once again – the wavefront is thus flat again. This allows for example to focus the pulse 8 and to easily detect it with a detector 9. The detector 9 is preferably adapted to carry out single photon counting. This can for example be done using an APD. On the other hand, if it was not the correct PUF 5 that was presented to the verifier 30, the action of the response transformation means 7 on the presented response 6 will still be to generate a wavefront with a random shape. There is no phase coincidence along this wavefront. Therefore, it is not possible to focus such a wavefront to a single point again, and consequently the applied single photon counting detector 9 will not count a sufficient number of photons.

The experimental setup shown in Fig. 3 therefore allows to reach two different aims: On the one hand, when a physical entity is presented as a PUF 5 to the verifier 30, it can be determined whether the correct PUF 5 is presented. On the other hand, the verifier 30 cannot be fooled by an emulation device, since it is physically impossible to read out the presented challenge 3, because the extent of information included in the challenge 3 is so high that it cannot be read out completely by performing a measurement (the number of photons in the challenge is smaller than the number of channels in the challenge creating means). Therefore, the experimental setup depicted in Fig. 3 is quantum secure.

One could of course think about some attempts to attack the security of the described invention. However, they will be hardly successful: It is for example possible that an attacker can send much more light into the inventive device than the device normally uses. Then several photons might be counted in the detector without use of the correct PUF. This scenario is simply prevented by adding additional "background" detectors to the inventive device which measure (for example via a beam splitter) how much light was incident on SLM 2 or, better, how much light fell outside of the pinhole/ the device.

In principle, the invention is also secure against holographic attacks. Without going into deep detail, this kind of attacks can be prevented by limiting the coherence length of the light source to a few times the mean free path of the PUF, i.e. a few 10 micrometers in the explicitly described embodiment of Fig. 3.

Fig. 4 shows a schematic experimental setup for defining valid CRPs. The light from a diode laser (not shown) enters a beam splitter 4a and is divided into two different light paths. The first light path is shown on the upper half in Fig. 4, and the second light path 20 is used as a reference light path 20 is found on the bottom half in Fig. 4. In the first light path, there are provided once again an SLM 2, a PUF 5 and an SLM 7. The SLM 2 acts as a challenge creating means, and the SLM 7 acts as a response transformation means. In the depicted example, the PUF 5 interacts with the presented light in a transmissive mode. However, of course, the transmission can be replaced by a reflection. The light entering the reference light path 20 is reflected by mirror 16 and once again by mirror 17. It then enters another beam splitter 4b, in which light from the two light paths is recombined and sent to a detector 13. Reference signs 1, 3, 6 and 8 depict in a schematic manner the wavefront shape due to interaction with SLM 2, PUF 5 and SLM 7. In the depicted example, the PUF 5 is represented as a layer of ZnO on glass.

The action of the experimental setup depicted in Fig. 4 is now as follows: Before the verification can start, the PUF 5 has to be characterized once. To this end, it is chosen a challenge wavefront with SLM 2. In the presented example, the challenges are binary phase challenges with a phase of 0 or pi, respectively. The amplitude and phase of the wavefront coming back from the PUF 5 is measured with an interferometric method and amounts of light from a CW diode laser are sampled (coherent OBIS 785nm LX). SLM 7 is set to act as a mirror with a flat phase. By moving the mirror 17 in the reference arm 20 with a piezo, the optical path length of the reference arm 20 can be varied, effectively changing its phase by pi. This results in the speckle pattern of the CCD 13 to show a cosine behavior as the function of the position of the mirror 17 in the reference arm 20, allowing to determine the phase of all the visible speckles. The information on the response wavefront is used to null the phase of a light from the PUF 5 by applying the conjugate phase with SLM 7. It is verified that as a result, all speckles on the CCD 13 now vary in phase with the piezo motion.

Next, the reference arm 20 of the interferometer is blocked, and with a flip mirror the CCD 13 is now replaced with a lens focusing the flat-wave front speckle pattern onto a camera 15 in the focal plane of the lens. Here it is observed that about 50% of the power is in the central spot. For the final demonstration, the CW laser diode light is dimmed and chopped in 500 ns long weak pulses. The CCD camera is replaced by a small pinhole and a single-photon counting Avalanche photodiode APD behind the pinhole.

An exemplary measurement result is depicted in Fig. 5: In Fig. 5a), the detected voltage V detected with the APD is depicted. The time interval of interest is determined using a time gate signal 10. The detection signal 11 comprises three high and well-defined peaks 12, the APD therefore counting three photons in the time interval of interest.

In the case depicted in Fig. 5a), a correct challenge response pair (the correct PUF) was applied, and then three photons were counted. In contrast thereto, the result depicted in Fig. 5b) corresponds to a case in which the challenge response pair was not valid (the wrong PUF was presented), for example; in the present case, for demonstration purposes, the settings of the challenge creating means (SLM 2) and the response transformation means (SLM 7) remained unchanged, but another part of PUF was chosen, thus presenting a "false" PUF. In this case, no photon could be detected with the APD.

Repeating the measurement 1000 times for an excitation power of approximately 250 photons in the challenge wavefront it was found an average 3.5 ± 1 detector clicks per pulse

for the correct challenge. The false negative rate (no click for correct challenge) was 0.6%, false positive rate (one click for wrong challenge) is 1%.

Fig. 6a) exemplarily illustrates a setting for a challenge sent to a PUF and Fig. 6b) shows the corresponding detection result for a correct PUF, whereas Fig. 6c) shows the detection result for a false PUF. In more detail, Fig. 6b) and c) show the light intensity behind the response-verifying means detected with a CCD. As can be seen, the light intensity in the (encircled) spot in the middle of the CCD is much higher in case a correct PUF is used than in the case in which a wrong PUF was presented the verifier.

The present invention provides for the first time a device and system as well as a method for verifying challenge-response pairs using a PUF being quantum secure, but at the same time avoiding problems typically arising when operating with fragile quantum states. With the help of the present invention, it cannot only be determined whether the PUF presented to the verifier is the correct key, but it is in principle impossible to replace the physical PUF by an emulation means and to thereby fool the verifier. According to the disclosed invention, this security is even realized "hands-off", e.g. it is not necessary to give away the PUF for (separately) checking whether it is a real physical entity of the expected type.

The present invention will be of high importance in the field of secure communication and authorization and can in particular be applied in authorization cards or payment cards, such as credit cards. Furthermore, the present invention can be used in connection with the topic of quantum key exchange using a PUF in quantum cryptography protocols.

List of reference signs

1	laser pulse
2	challenge creating means (SLM)
3	challenge
4	beam splitter
5	PUF
6	response
7	response transformation means (SLM)
8	laser pulse
9	detector
10	time gating signal

11 APD signal
12 Peak
13 CCD
15 pinhole or APD
16 mirror
17 mirror
20 reference arm
30 verifier
40 box

List of Scientific References

01. Pappu, R.: *Physical One-Way Functions.* PhD thesis, MIT (2001)
02. Pappu, R., Recht, B., Taylor, J., Gershenfeld, N.: *Physical One-Way Functions.* Science 297, 2026–2030 (2002)
03. Gassend, B., Clarke, D.E., van Dijk, M., Devadas, S.: *Silicon physical unknown functions. In: ACM Conf. on Computer and Communications Security – CCS 2002,* November 2002, pp. 148–160 (2002)
04. Tuyls, P., Schrijen, G.J., Škorić, B., van Geloven, J., Verhaegh, R., Wolters, R.: *Read-proof hardware from protective coatings.* In: Goubin, L., Matsui, M. (eds.) CHES 2006. LNCS, vol. 4249, pp. 369–383. Springer, Heidelberg (2006)
05. Kirovski, D.: *Toward an automated verification of certificates of authenticity. In: ACM Conference on Electronic Commerce*, pp. 160–169. ACM, New York (2004)
06. DeJean, G., Kirovski, D.: *Radio frequency certificates of authenticity.* In: IEEE Antenna and Propagation Symposium – URSI (2006)
07. Škorić, B., Bel, T., Blom, A.H.M., de Jong, B.R., Kretschman, H., Nellissen, A.J.M.: *Randomized resonators as uniquely identifiable anti-counterfeiting tags.* In: Secure Component and System Identification Workshop, Berlin (March 2008)
08. Buchanan, J.D.R., Cowburn, R.P., Jausovec, A., Petit, D., Seem, P., Xiong, G., Atkinson, D., Fenton, K., Allwood, D.A., Bryan, M.T.: *Forgery: 'fingerprinting' documents and packaging.* Nature, Brief Communications 436, 475 (2005)
09. Guajardo, J., Kumar, S.S., Schrijen, G.J., Tuyls, P.: *FPGA intrinsic PUFs and their use for IP protection.* In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 63–80. Springer, Heidelberg (2007)
10. Kumar, S.S., Guajardo, J., Maes, R., Schrijen, G.J., Tuyls, P.: *The Butterfly PUF: Protecting IP on every FPGA.* In: HOST 2008, pp. 67–70. IEEE, Los Alamitos (2008)

11. Chong, C.N., Jiang, D., Zhang, J., Guo, L.: *Anti-counterfeiting with a random pattern*. In: SECURWARE 2008, pp. 146–153. IEEE, Los Alamitos (2008)

12. Kursawe, K., Sadeghi, A.-R., Schellekens, D., Škorić, B., Tuyls, P.: *Reconfigurable physical unclonable functions*. In: HOST 2009 (2009)

13. Škorić, B.: *Quantum Readout of Physical Unclonable Functions*, AFRICACRYPT 2010, LNCS 6055, pp. 369–386 (2010)

14. Vellekoop, I.M., Mosk, A.P.: *Focusing coherent light through opaque strongly scattering media*, Optics Lett. 32, No. 16, pp. 2309 – 2311 (2007)

15. Vellekoop, I.M., Mosk, A.P.: *Phase control algorithms for focusing light through turbid media*, Optics Communications 281, pp. 3071-3080 (2008)

Claims

1. A device (30) for verifying challenge-response pairs, comprising:
   - a wave source, in particular a light source;
   - a challenge creating means (2) for creating a challenge (3), in particular an optical challenge (3), to be sent to a PUF (5), in particular when receiving waves emitted from the wave source;
   - a response transformation means (7) for verifying a response from a PUF (5); and
   - a detector (9) for reading out the result of the verification carried out by the response transformation means (7).

2. The device (30) according to claim 1, wherein the number of interaction particles, in particular photons, in the challenge (3) is less than the number of parameters needed to fully describe a setting of the challenge creating means (2).

3. The device (30) according to any one of the preceding claims, wherein the device (30) is adapted to distinguish a positive result for verification from a negative result for verification based on a preselected number of interaction particles, in particular photons, detected / detectable in the detector (9) for one challenge-response pair.

4. The device (30) according to any one of the preceding claims, wherein the nature of the response transformation means (7) is of the same type as that of the challenge creating means (2).

5. The device (30) according to any one of the preceding claims, wherein the action of the response transformation means is of the type of a reversion or inversion or projection and reverses or inverts or projects the response.

6. The device (30) according to any one of the preceding claims,
   - wherein the wave source is a light source and wherein the interaction particles are photons;
   - wherein a challenge and/or a response is defined by a physical property of photons, in particular phase information, amplitude information, polarization information, frequency information, spatial information and/or time information of a photon; and
   - wherein the challenge and/or response is in partiular described by: a spatial distribution, in particular a two dimensional distribution, of the physical property of

photons, a frequency distribution of the physical property of photons and / or a time distribution of the physical property of photons.

7. The device (30) according to any one of the preceding claims, wherein the challenge creating means (2) or/and the response transformation means (7) is/are adapted to carry out wavefront shaping on provided light.

8. The device (30) according to the preceding claim, wherein the challenge creating means (2) or/and the response transformation means (7) is/are spatial light modulators for manipulating the phase and/or amplitude of light.

9. The device (30) according to any one of the preceding claims, wherein the wave source is a laser adapted to emit pulses of a limited number of photons.

10. The device (30) according to any one of the preceding claims, wherein a focusing means is provided for focusing waves onto the detector (9) for detection.

11. The device (30) according to any one of the preceding claims, wherein the spatial detection range of the detector (9) is point-like or/and the detector (9) is adapted to carry out single interaction-particle counting, in particular single-photon counting.

12. The device (30) according to the preceding claim, wherein the detector (9) is an avalanche photodiode.

13. A system for verifying challenge-response pairs, comprising:
- the device (30) according to any one of claims 1 to 12; and
- a PUF (5) means.

14. The system according to the preceding claim, wherein the PUF (5) is adapted to act on the basis of scattering, in particular light scattering, either in transmission or in reflection operation mode.

15. A method for verifying challenge-response pairs, comprising the following steps:
- emitting a wave, in particular light;
- creating a challenge (3), in particular an optical challenge (3), in particular by directing the emitted wave onto a challenge creating means (2);
- sending the challenge (3) to a PUF (5) means, thereby creating a response (6), in

particular an optical response, to the challenge (3);
- verifying the response by directing the response (6) onto a response transformation means for verification (7); and
- reading out the result of verification carried out by the response transformation means (7) with a detector (9).

16. The method according to the preceding claim, wherein the number of interaction particles, in particular photons, in the challenge (3) is less than the number of parameters needed to fully describe the setting of the challenge creating means (2).

17. The method according to any one of claims 15 to 16, wherein the step of reading out the verification result comprises the step of interaction particle counting, in particular photon counting.

18. The method according to any one of claims 15 to 17, wherein the challenge creating means and/or the response transformation means are adapted to carry out wavefront shaping.

19. The method according to any one of claims 15 to 18, wherein the method is executed applying a system according to any one of claims 13 to 14.

AMENDED CLAIMS
received by the International Bureau
on 21 November 2013 (21.11.2013)

1. A device (30) for verifying challenge-response pairs, comprising:
   - a coherent light source;
   - a wavefront shaping means (2) for creating an optical challenge (3) to be sent to a PUF (5) when receiving light emitted from the light source;
   - a wavefront shaping means (7) for verifying an optical response (6) from a PUF (5);
   - a detector (9) for reading out the result of the verification carried out by the wavefront shaping means (7) for verifying the response (6); and
   - a focusing means wherein the focusing means focuses light onto the detector (9) for detection.

2. The device (30) according to claim 1, wherein the number of photons in the challenge (3) is less than the number of parameters needed to fully describe a setting of the wavefront shaping means (2) for creating the challenge (3).

3. The device (30) according to any one of the preceding claims, wherein the device (30) is adapted to distinguish a positive result for verification from a negative result for verification based on a preselected number of photons detected / detectable in the detector (9) for one challenge-response pair.

4. The device (30) according to any one of the preceding claims, wherein the action of the wavefront shaping means (7) for verifying the optical response (6) is of the type of a reversion or inversion or projection and reverses or inverts or projects the response (6).

5. The device (30) according to any one of the preceding claims,
   - wherein the challenge and/or the response is defined by a physical property of photons, in particular phase information, amplitude information, polarization information, frequency information, spatial information and/or time information of a photon; and
   - wherein the challenge and/or response is described by: a spatial distribution, in particular a two dimensional distribution, of the physical property of photons, a

frequency distribution of the physical property of photons and / or a time distribution of the physical property of photons.

6. The device (30) according to the preceding claim, wherein the wavefront shaping means (2) for creating the challenge (3) or/and the wavefront shaping means (7) for verifying the response (6) is/are spatial light modulators for manipulating the phase and/or amplitude of light.

7. The device (30) according to any one of the preceding claims, wherein the coherent light source is a laser adapted to emit pulses of a limited number of photons.

8. The device (30) according to any one of the preceding claims, wherein the spatial detection range of the detector (9) is point-like or/and the detector (9) is adapted to carry out single-photon counting.

9. The device (30) according to the preceding claim, wherein the detector (9) is an avalanche photodiode.

10. A system for verifying challenge-response pairs, comprising:
- the device (30) according to any one of claims 1 to 9; and
- a PUF (5) means.

11. The system according to the preceding claim, wherein the PUF (5) is adapted to act on the basis of light scattering, either in transmission or in reflection operation mode.

12. A method for verifying challenge-response pairs, comprising the following steps:
- emitting coherent light;
- creating an optical challenge (3) by directing the emitted light onto a wavefront shaping means (2);
- sending the challenge (3) to a PUF (5) means, thereby creating an optical response (6) to the challenge (3);
- verifying the response (6) by directing the response (6) onto a wavefront shaping means for verification (7); and
- reading out the result of verification carried out by the wavefront shaping means for verification (7) with a detector (9), wherein light is focused onto the detector (9) for detection.

13. The method according to the preceding claim, wherein the number of photons in the challenge (3) is less than the number of parameters needed to fully describe the setting of the wavefront shaping means (2) for creating the challenge (3).

14. The method according to any one of claims 12 to 13, wherein the step of reading out the verification result comprises the step of photon counting.

15. The method according to any one of claims 12 to 14, wherein the method is executed applying a system according to any one of claims 10 to 11.

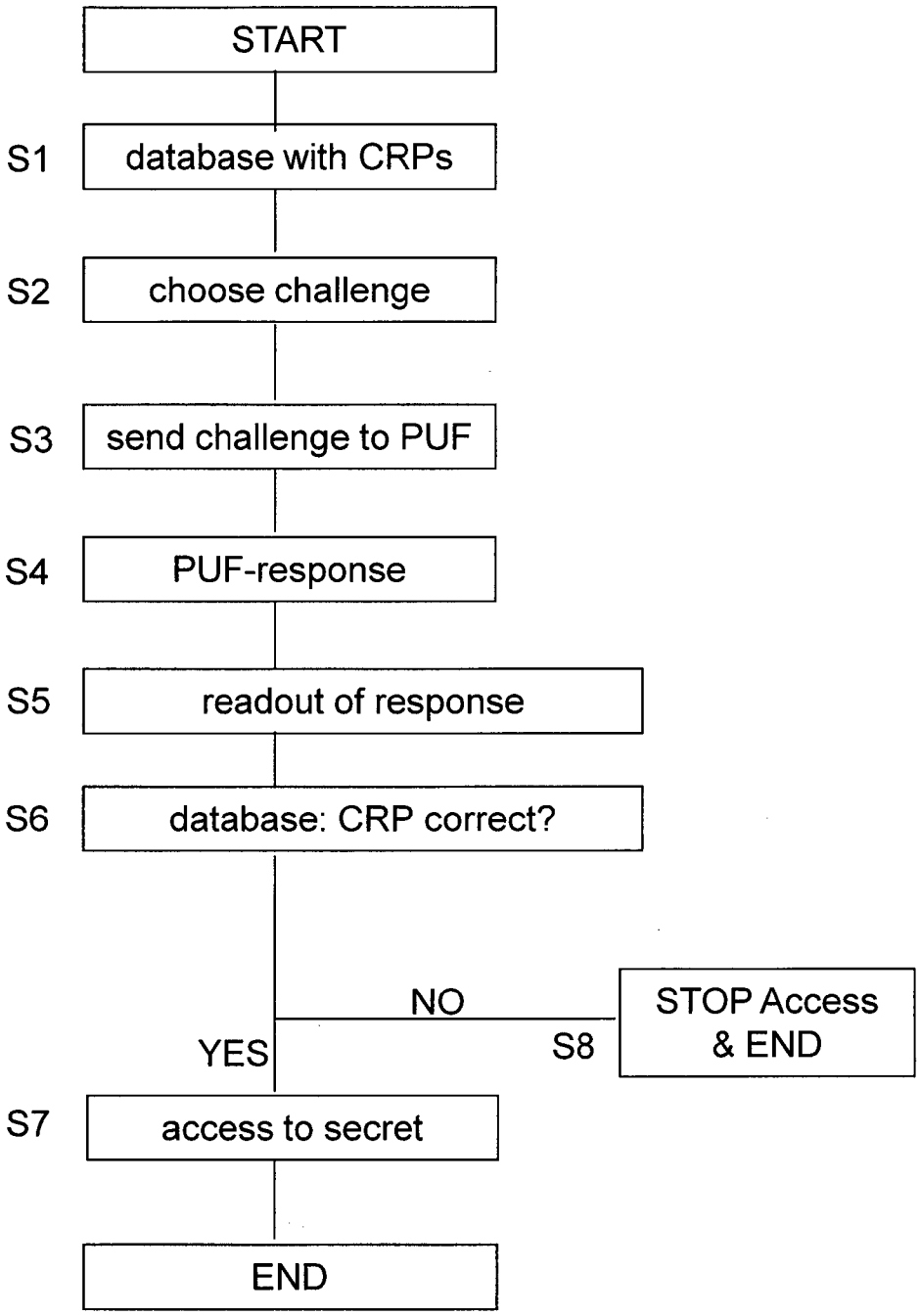

START
S1
database with CRPs
S2
choose challenge
S3
send challenge to PUF
S4
PUF-response
S5
readout of response
S6
database: CRP correct?
NO
S8
STOP Access & END
YES
S7
access to secret
END

Fig. 1

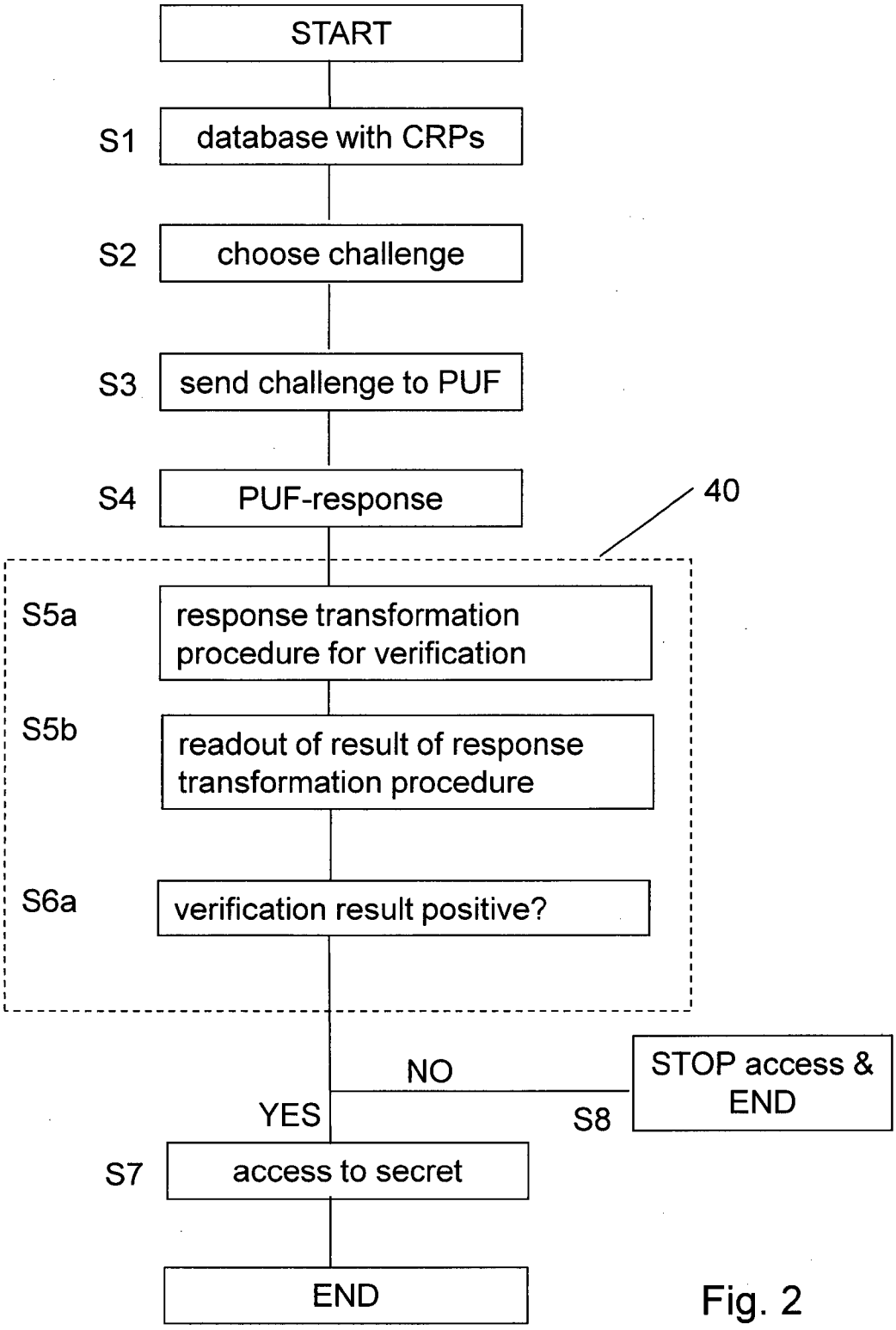

START
S1
database with CRPs
S2
choose challenge
S3
send challenge to PUF
S4
PUF-response
40
S5a
response transformation procedure for verification
S5b
readout of result of response transformation procedure
S6a
verification result positive?
NO
STOP access & END
S8
YES
S7
access to secret
END

Fig. 2

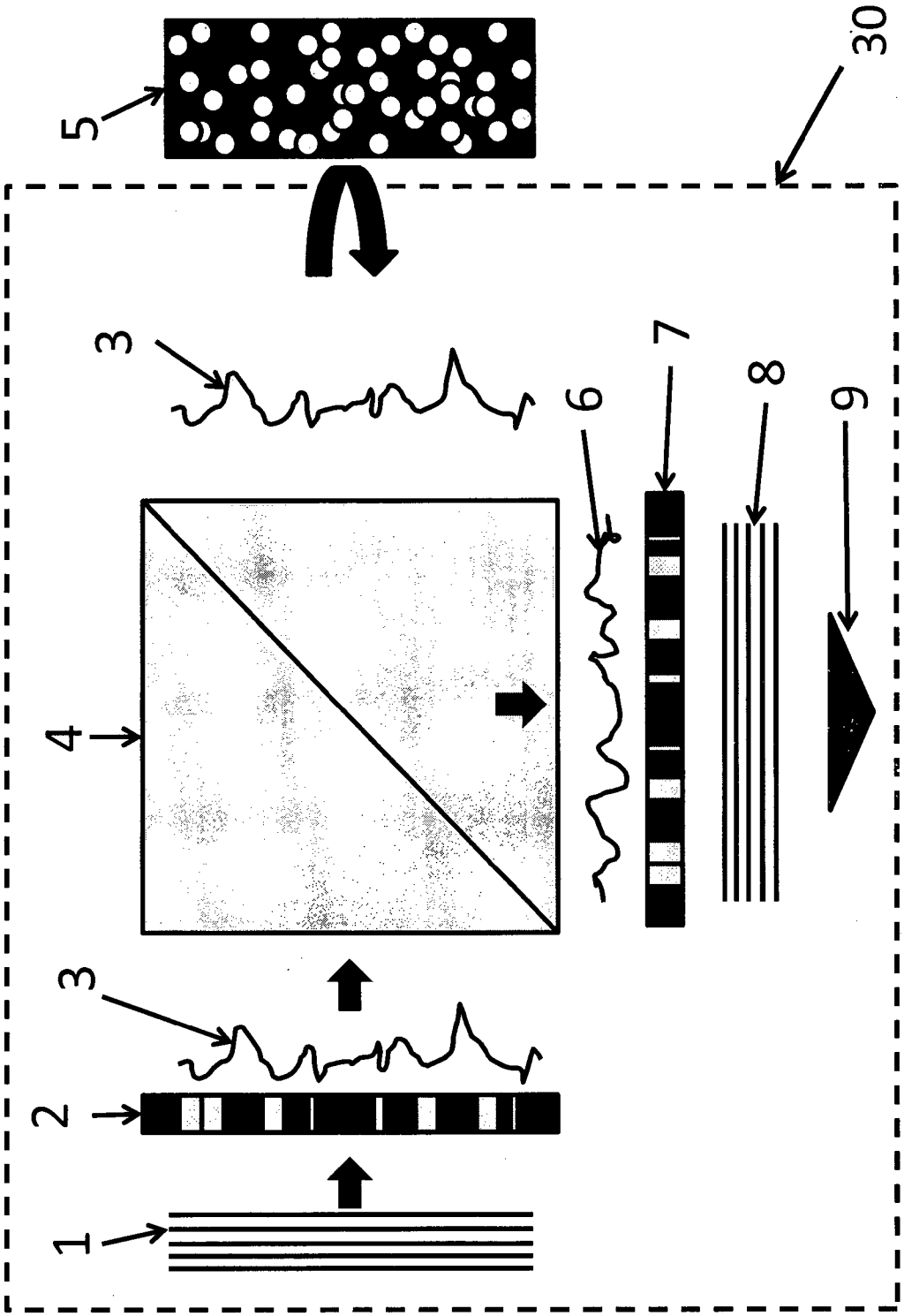


Fig. 3

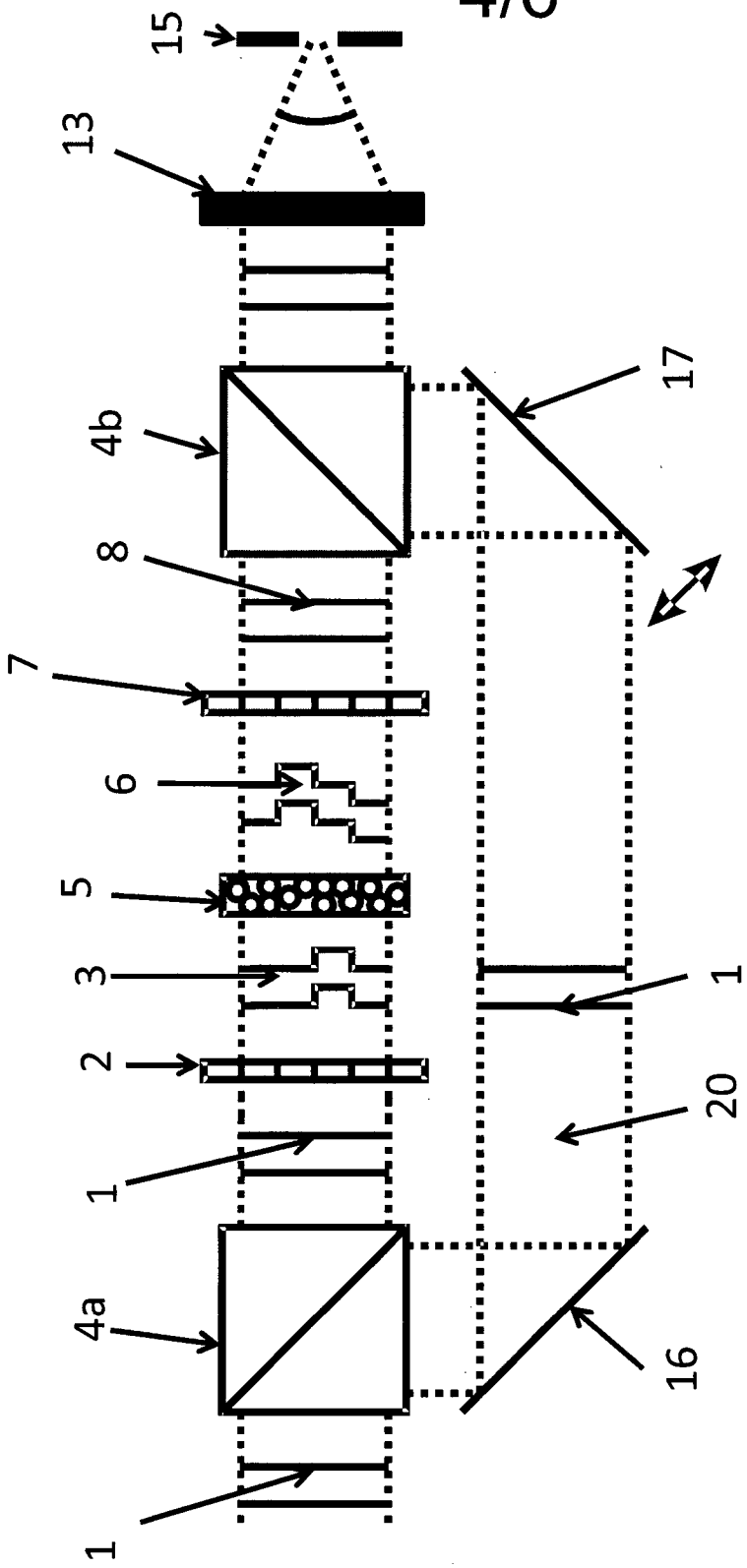


Fig. 4

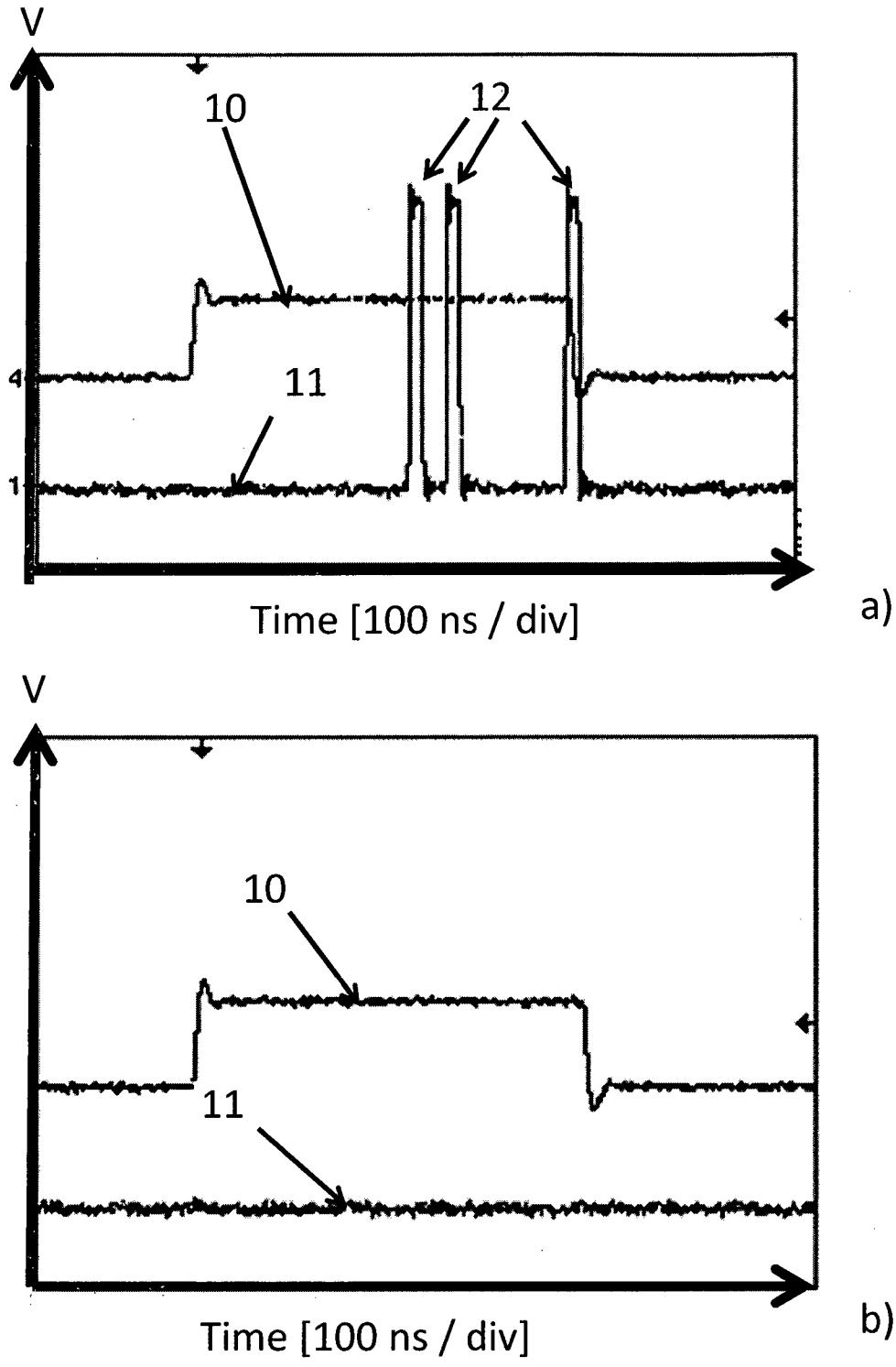
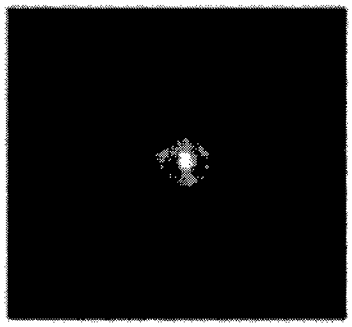


Fig. 5

a)

b)



c)

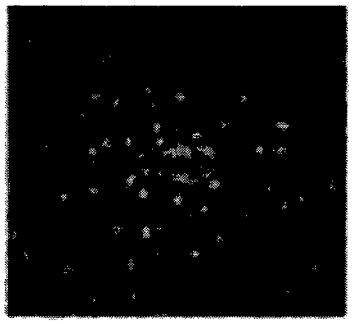


Fig. 6

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2013/002249

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/32
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2008/121708 A1 (RHOADS GEOFFREY B [US] ET AL) 29 May 2008 (2008-05-29) abstract; claims 1,5-7,10-12; figures 2,4,7,11 paragraphs [0041] - [0045], [0059] - [0061], [0064] - [0070], [0158] - [0161], [0171] - [0180]	1-19

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 September 2013	23/09/2013

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Wolters, Robert

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2013/002249

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2007/046018 A1 (KONINKL PHILIPS ELECTRONICS NV [NL]; OPHEY WILLEM G [NL]; SKORIC BORIS) 26 April 2007 (2007-04-26) cited in the application abstract; claims 1,12-14,17-19; figures 1-3 page 1, line 5 - page 2, line 4 page 3, line 9 - line 27 page 4, line 8 - line 29 page 5, line 13 - page 6, line 3 page 8, line 1 - line 7 page 8, line 21 - page 10, line 20	1-19
X	WO 98/28707 A1 (INTEL CORP [US]) 2 July 1998 (1998-07-02) abstract; claims 1,2,7,15,21; figures 1-3 page 5, line 9 - page 8, line 21	1-19
A	VELLEKOOP J M ET AL: "FOCUSING COHERENT LIGHT THROUGH OPAQUE STRONGLY SCATTERING MEDIA", OPTICS LETTERS, OSA, OPTICAL SOCIETY OF AMERICA, WASHINGTON, DC, US, vol. 32, no. 16, 15 August 2007 (2007-08-15), pages 2309-2311, XP001506776, ISSN: 0146-9592, DOI: 10.1364/OL.32.002309 cited in the application the whole document	1-19
A	VELLEKOOP I M ET AL: "Phase control algorithms for focusing light through turbid media", OPTICS COMMUNICATIONS, NORTH-HOLLAND PUBLISHING CO. AMSTERDAM, NL, vol. 281, no. 11, 1 June 2008 (2008-06-01) , pages 3071-3080, XP022608018, ISSN: 0030-4018, DOI: 10.1016/J.OPTCOM.2008.02.022 [retrieved on 2008-03-10] cited in the application the whole document	1-19
A	WO 2005/059629 A1 (KONINKL PHILIPS ELECTRONICS NV [NL]; STALLINGA SJOERD [NL]; SKORIC BOR) 30 June 2005 (2005-06-30) cited in the application abstract; claims 1,7,16 page 1, line 20 - page 2, line 11 page 2, line 33 - page 3, line 6	1-19

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2013/002249

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2008121708 A1	29-05-2008	US 2008121708 A1	29-05-2008
		US 2012273570 A1	01-11-2012
WO 2007046018 A1	26-04-2007	CN 101292465 A	22-10-2008
		CN 101292466 A	22-10-2008
		EP 1941652 A1	09-07-2008
		JP 2009511976 A	19-03-2009
		US 2008231418 A1	25-09-2008
		WO 2007046018 A1	26-04-2007
WO 9828707 A1	02-07-1998	AU 5610298 A	17-07-1998
		DE 69723474 D1	14-08-2003
		DE 69723474 T2	24-12-2003
		EP 0966722 A1	29-12-1999
		JP 4271734 B2	03-06-2009
		JP 2001507488 A	05-06-2001
		US 5933502 A	03-08-1999
		WO 9828707 A1	02-07-1998
WO 2005059629 A1	30-06-2005	CN 1890595 A	03-01-2007
		EP 1695136 A1	30-08-2006
		JP 4448139 B2	07-04-2010
		JP 2007519944 A	19-07-2007
		KR 20060123278 A	01-12-2006
		US 2007090312 A1	26-04-2007
		WO 2005059629 A1	30-06-2005