(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
3. April 2014 (03.04.2014)

WIPO | PCT

(10) Internationale Veröffentlichungsnummer
WO 2014/048631 A1

(51) Internationale Patentklassifikation:
G06F 21/57 (2013.01) *G06F 11/27* (2006.01)
G01R 31/3187 (2006.01) *H04L 9/32* (2006.01)

(21) Internationales Aktenzeichen: PCT/EP2013/066653

(22) Internationales Anmeldedatum:
8. August 2013 (08.08.2013)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2012 217 716.7
28. September 2012 (28.09.2012) DE

(71) Anmelder: **SIEMENS AKTIENGESELLSCHAFT** [DE/DE]; Wittelsbacherplatz 2, 80333 München (DE).

(72) Erfinder: **FALK, Rainer**; Primelweg 9, 85586 Poing (DE).

(81) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare nationale Schutzrechtsart)*: 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, SA, 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) Bestimmungsstaaten *(soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, RU, TJ, TM), europäisches (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).

Veröffentlicht:

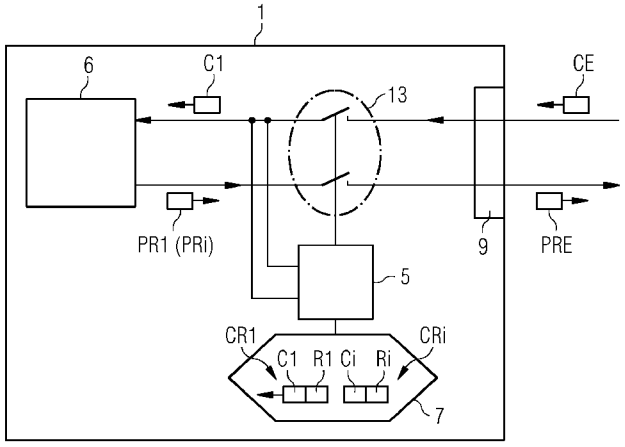
— *mit internationalem Recherchenbericht (Artikel 21 Absatz 3)*

WO 2014/048631 A1

(54) **Title**: SELF-TEST OF A PHYSICAL UNCLONABLE FUNCTION

(54) **Bezeichnung** : SELBST-TEST EINER PHYSICAL UNCLONABLE FUNCTION

FIG 3



(57) **Abstract**: The invention relates to a circuit unit (1) comprising a Physical Unclonable Function (6), hereinafter referred to as PUF (6), a verification unit (5) and an information storage device (7) for storing at least one Challenge-Response-Pair (CR1); wherein the Challenge-Response-Pair (CR1) comprises a Challenge Information (C1) and a Response Information (R1) associated therewith, and wherein the verification unit (5) is embodied and/or adapted, in order to bring about an input of the challenge information (C1) into the PUF (6) and to use a PUF Response (PR1) created thereafter by the PUF (6) and the Response Information for a comparison, and in dependence of the result of the comparison release or restrict a use of the PUF (6).

(57) **Zusammenfassung**:

[Fortsetzung auf der nächsten Seite]

Schaltkreiseinheit (1) umfassend eine im Folgenden PUF (6) genannte Physical Unclonable Function (6), eine Prüfeinheit (5) und einen Informationsspeicher (7) zum Speichern mindestens eines Challenge-Response-Paares (CR1); wobei das Challenge-Response-Paar (CR1) eine Challenge-Information (C1) und eine dazu gehörige Response-Information (R1) umfasst; und wobei die Prüfeinheit (5) ausgestaltet und/oder adaptiert ist, eine Eingabe der Challenge-Information (C1) in die PUF (6) zu veranlassen, und eine darauf durch die PUF (6) erzeugte PUF-Response (PR1) und die Response-Information (R1) für einen Vergleich zu verwenden und abhängig vom Ergebnis des Vergleichs eine Verwendung der PUF (6) freizugeben oder einzuschränken.

Beschreibung

Selbst-Test einer Physical Unclonable Function

Die vorliegende Erfindung bezieht sich auf das technische Gebiet der Selbsttests von Physical Unclonable Functions.

PUF-based Secure Test Wrapper Design for Cryptographic SoC Testing
http://www.cosic.esat.kuleuven.be/publications/article-2165.pdf beschreibt die Verwendung einer PUF, um den Zugriff zu einer Test-Schnittstelle eines ICs zu schützen. Erwähnt wird auch der allgemein bekannte Selbst-Test (BIST - built-in self test), durch den eine Baugruppe selbst ihre korrekte Funktionalität testet und eine entsprechende Status-Meldung bereitstellt.

Von Tim Tuyls, Boris Skoric: Strong Authentication with Physical Unclonable Functions, in Security Privacy, and Trust in Modern Data Management, Springer, 2007, p.133ff. ist bekannt, aus einer PUF einen Sensor zum Erkennen von physikalischen Manipulationen /Tampering) zu bauen. Dazu überwacht die PUF im Betrieb, ob auf bekannte Challenges die erwarteten Response-Werte zurückgeliefert werden. Eine physikalischen Manipulation, bei der die PUF physikalisch zerstört oder modifziert wird, kann erkannt werden, indem nicht mehr die erwartete Response breitgestellt wird (siehe Seite 135, wo beschrieben wird, dass real time tamper Detektierung erreicht werden kann, wenn die PUF eine integrierte PUF ist, welche Zugang auf die Enrolment-Daten hat). Die PUF führt dann regulär Selbsttests aus und nimmt die angemessene Handlung vor, z.B. Auslösen eines Alarms oder Ausschalten, sobald eine Response nicht mit den Enrolement-Daten übereinstimmt.

Figur 1 zeigt eine Physical Unclonable Function 105, oft auch einfach PUF genannt, gemäß dem Stand der Technik. Eine Challenge-Information C105 ist die PUF eingebbar. Die PUF 105 generiert daraufhin eine Response-Information R105.

Eine PUF kann auch zur Bildung eines kryptographischen Schlüssels verwendet werden. Figur 2 zeigt ein entsprechendes Grundschema nach dem Stand der Technik mit einer PUF 115, in welche eine Challenge-Information C115 eingebbar ist, worauf die PUF 115 eine Response-Information R115 ausgibt. Dabei wird durch einen Fuzzy Key Extractor 118, auch FKE genannt, unter Verwendung von Hilfs-Daten 117 mittels der PUF 115 ein kryptographischer Schlüssel CK bestimmt.

Einen Überblick über Physical Unclonable Functions (PUF) geben die Vorlesungsunterlagen http://www.sec.in.tum.de/assets/lehre/ss10/sms/sms-kap6-rfid-teil2.pdf.

Physical Unclonable Functions sind bekannt, um Objekte zuverlässig anhand ihrer intrinsischen physikalischen Eigenschaften zu identifizieren. Eine physikalische Eigenschaft eines Gegenstandes (z.B. ein Halbleiter-IC) wird dabei als individueller „Fingerabdruck" verwendet. Die Authentisierung eines Objekts basiert darauf, dass abhängig von einem Challenge-Wert durch eine durch physikalische Eigenschaften definierte PUF-Funktion ein zugehöriger Response-Wert zurückgeliefert wird. Physical Unclonable Functions (PUF) bieten eine flächensparende und damit kostengünstige Möglichkeit, ein physikalisches Objekt anhand seiner intrinsischen physikalischen Eigenschaften zu authentisieren. Dazu wird zu einem vorgegebenen Challenge-Wert durch die PUF abhängig von objektspezifischen physikalischen Eigenschaften des Objekts ein zugehöriger Response-Wert ermittelt. Ein Prüfer, der ein Objekt authentisieren möchte, kann bei bekannten Challenge-Response-Paaren durch einen Ähnlichkeitsvergleich der vorliegenden und der vom authentisierten Objekt bereitgestellten Response-Werten das Objekt als Originalobjekt identifizieren.
Weitere Anwendungen einer PUF sind bekannt, insbesondere die Chip-interne Bestimmung eines kryptographischen Schlüssels mittels einer PUF.

Beispiele für PUFs sind Delay-PUF / Arbiter-PUF, SRAM-PUF, Ring-Oscillator PUF, Bistable Ring PUF, Flip-Flop-PUF, Glitch PUF, Cellular Non-linear Network PUF, oder Butterfly-PUF.

Spezielle PUFs z.B. bei ICs können auf dem IC aufgebracht werden (Coating PUF, Optical PUF) und dadurch eine Schicht oberhalb des ICs realisieren, die zum einen den Zugriff auf interne (darunterliegende) Strukturen verhindert, und die bei Entfernen zerstört wird. Dies hat jedoch den Nachteil, dass spezielle Fertigungsverfahren benötigt werden. Auch werden ggf. Angriffe, die die Schutzschicht nicht beschädigen, nicht erkannt (z.B. die von der gegenüberliegenden Seite oder seitlich erfolgen).

Die PUF-Rohdaten (Response) müssen im Allgemeinen noch nachbearbeitet werden, um statistische Schwankungen der PUF-Response zu kompensieren (z.B. durch eine Vorwärtsfehlerkorrektur oder durch eine Merkmalsextraktion entsprechend wie bei einer herkömmlichen Fingerabdrucks-Authentisierung). Dies ist auch unter dem Begriff "Fuzzy Key Extractor" bekannt (siehe z.B. http://www.iacr.org/archive/eurocrypt2004/30270518/DRS-ec2004-final.pdf ; http://www.cs.ucla.edu/~rafail/PUBLIC/89.pdf).

Es ist bekannt, die Implementierung eines Crypto-Algorithmus durch einen unabhängigen Prüfer zu verifizieren, z.B. Cryptographic Algorithm Validation Program (CAVP), siehe z.B. http://csrc.nist.gov/groups/STM/cavp/index.html und http://www.atsec.com/us/cryptographic-algorithm-testing-lab-resources.html

Es ist bekannt, dass ein Gerät einen Selbsttest durchführt. Im Speziellen ist bekannt, dass bei einem Gerätestart und/oder wiederkehrend ein Selbst-Check der Crypto-Funktionalität erfolgt. Nur im positiven Fall wird die Nutzung der Crypto-Funktionalität freigegeben. Siehe z.B. http://spiderman-

2.laas.fr/WDSN08/2ndWDSN08(LAAS)_files/Texts/WDSN08-08-DiNatale.pdf zum Ressourcen-effizienten Built-in self test eines symmetrischen Crypto-Algorithmus. Auch fordern manche Standards wie FIPS140-2 einen Selbst-Test der Crypto-Funktionen (siehe http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf Abschnitt 4.9). Bekannte Verfahren sind in FIPS140-2 Abschnitt 4.9 angegeben.

Bei physikalischen Zufallszahlengeneratoren ist eine Evaluierung mittels statistischer Tests bekannt (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/ais31_pdf.pdf?__blob=publicationFile). Es ist bekannt, die Qualität der physikalisch erzeugten Zufallszahlen im laufenden Betrieb zu testen und im Fehlerfall die Bereitstellung von Zufallszahlen einzustellen (http://www.ibbergmann.org/Physikalischer_Zufallssignalgenerator.pdf)

Es ist bekannt, auf einer PUF einen Schlüssel abzuleiten. Auch bei statistischen Schwankungen kann durch Fehlerkorrekturverfahren der Schlüssel eindeutig erzeugt werden (http://members.home.nl/skoric/security/PUF_KeyExtraction.pdf). Dabei ist auch beschrieben, einige Challenge-Werte zu reservieren, um damit eine Kalibrierung der PUF vorzunehmen. Ein Überprüfer (Verifier) prüft anhand dieser bekannten Kalibrierwerte, ob der Leser (Überprüfer) und die PUF korrekt ausgerichtet sind. Nur bei hinreichend geringer Abweichung der gemessenen und der gespeicherten Kalibrierwerte erfolgt eine tatsächliche Authentisierung. Dies betrifft speziell optische PUFs, bei denen ein Lesegerät und die optische PUF hinreichend genau ausgerichtet sein müssen, um das erwartete Ergebnis zu erhalten.

Es sind unterschiedliche Verfahren zur Fehlerkorrektur bzw. Fehlererkennung bekannt, z.B. BCH-Codes oder Turbo-Codes.

Diese können auch eingesetzt werden, um die Hamming-Distanz, d.h. die Anzahl abweichender Bits, zu ermitteln.

Es ist bewährte Praxis, dass eine kryptographische Security-Komponente im Betrieb einen Selbsttest durchführt, sodass sie bei einer Fehlfunktion nicht genutzt werden kann. Eine Physical Unclonable Function hat hier aufgrund ihres statistischen Verhaltens im Vergleich zu einem herkömmlichen kryptographischen Algorithmus besondere Anforderungen, sodass die bekannten Selbsttestverfahren nicht nutzbar sind.

Eine Physical Unclonable Function ist ein elementarer Security-Funktionsbaustein, mit dem z.B. eine Authentisierung erfolgen kann oder ein kryptographischer Schlüssel bestimmt werden kann.

Es besteht daher ein Bedarf an einer sicheren PUF. Es ist Aufgabe der vorliegenden Erfindung diesem Bedarf nachzukommen.

Diese Aufgabe wird durch die in den unabhängigen Ansprüchen beschriebenen Merkmalskombinationen gelöst. Vorteilhafte Ausgestaltungen der Erfindung sind in weiteren Ansprüchen ange¬geben.

Gemäß einem ersten Aspekt der Erfindung wird eine Schaltkreiseinheit vorgeschlagen. Die Schaltkreiseinheit umfasst eine Physical Unclonable Function (PUF), eine Prüfeinheit und einen Informationsspeicher zum Speichern mindestens eines Challenge-Response-Paares. Das Challenge-Response-Paar umfasst eine Challenge-Information und eine dazu gehörige Response-Information. Die Prüfeinheit ist ausgestaltet und/oder adaptiert, eine Eingabe der Challenge-Information in die PUF zu veranlassen und eine darauf durch die PUF erzeugte PUF-Response und die Response-Information für einen Vergleich zu verwenden. Abhängig vom Ergebnis des Vergleichs gibt die Prüfeinheit eine Verwendung der PUF frei oder schränkt diese ein.

Gemäß einem weiteren Aspekt betrifft die Erfindung ein Verfahren zum Durchführen eines Selbstests einer durch eine Schaltkreiseinheit umfassten PUF. Die Schaltkreiseinheit umfasst eine PUF, eine Prüfeinheit und einen Informationsspeicher zum Speichern mindestens eines Challenge-Response-Paares. Das Challenge-Response-Paar umfasst dabei eine Challenge-Information und eine dazu gehörige Response-Information. Im Rahmen des Verfahrens wird die Challenge-Information in die PUF eingegeben. Eine darauf durch die PUF erzeugte PUF-Response und die Response-Information werden durch die Prüfeinheit für einen Vergleich verwendet. Abhängig vom Ergebnis des Vergleichs wird eine Verwendung der PUF freigegeben oder eingeschränkt.

Bevorzugte Ausführungsformen der Erfindung werden nachfolgend anhand der Figuren beispielsweise näher erläutert. Dabei zeigen:

Figur 1 eine PUF gemäß dem Stand der Technik;

Figur 2 ein Grundschema nach dem Stand der Technik mit dem mittels einer PUF ein kryptographischer Schlüssel bestimmbar ist;

Figur 3 eine Schaltkreiseinheit gemäß einer bevorzugten Ausführungsform der Erfindung; und

Figur 4 ein Flussdiagramm für eine bevorzugte Ausführungsform des erfinderischen Verfahrens.

Figur 3 zeigt eine Schaltkreiseinheit 1 gemäß einer bevorzugten Ausführungsform der Erfindung. Die Schaltkreiseinheit 1 umfasst eine Physical Unclonable Function 6, eine Prüfeinheit 5 und einen Informationsspeicher 7 zum Speichern mindestens eines Challenge-Response-Paares CR1. Weitere Challenge-Response-Paare CRi können in dem Informationsspeicher 7 speicherbar sein. Die Physical Unclonable Function 6 wird im Fol-

genden auch PUF 6 genannt. Ein Challenge-Response-Paar CR1, respektive CRi umfasst typischerweise eine Challenge-Information C1, respektive Ci und eine dazu gehörige Response-Information R1, respektive Ri. Die Prüfeinheit 5 ist ausgestaltet und/oder adaptiert, eine Eingabe der Challenge-Information C1 oder mehrerer Challenge-Information Ci in die PUF 6 zu veranlassen. Die Prüfeinheit 5 ist ausgestaltet und/oder adaptiert, die darauf durch die PUF 6 erzeugte PUF-Response PR1 und die Response-Information R1 für einen Vergleich zu verwenden. Zudem ist die Prüfeinheit 5 ausgestaltet und/oder adaptiert abhängig vom Ergebnis des Vergleichs eine Verwendung der PUF 6 freizugeben oder einzuschränken. Die Freigabe, respektive Einschränkung der PUF 6, kann beispielsweise mittels eines in Figur 3 dargestellten Schalters 13 durchführbar sein.

Figur 3 zeigt also eine physikalische PUF 6, beispielsweise nach dem Stand der Technik und eine Prüfeinheit 5, die mittels gespeicherter Referenzdaten CR1, CRi die physikalische PUF 6 testet, bevor der Zugriff von Außen auf die PUF zugelassen wird (durch Schalter 13 symbolisch dargestellt).

Vorzugsweise ist die Schaltkreiseinheit 1 ein integrierter Schaltkreis 1. Dies erhöht die Angriffssicherheit. Denkbar ist, dass die Schaltkreiseinheit 1 aber auch eine Kombination von integrierten Schaltkreisen ist, die mit geeigneten Mitteln, zum Beispiel eingegossen in einen geeigneten Plastik oder sonstigen geeigneten Werkstoff eine dauerhafte Einheit bildet.

Vorzugsweise umfasst die Schaltkreiseinheit 1 eine Kommunikationsschnittstelle 9, durch welche ein Zugriff von extern durch ein externes Gerät auf die PUF 6 vornehmbar ist. Wie in Figur 9 dargestellt, kann bei einer freigegebenen Kommunikationsschnittstelle 9 eine externe Challenge-Information CE mittels der Kommunikationsschnittstelle 9 in die PUF 6 eingegeben werden. Die PUF 6 gibt darauf hin eine für extern be-

stimmte PUF-Response PRE für das externe Gerät via die Kommunikationsschnittstelle 9 aus.

Vorzugsweise ist die Verwendung der PUF 6 freigebbar oder einschränkbar, indem der Zugriff auf die PUF 6 direkt freigegeben oder gesperrt wird. Dabei kann beispielsweise die Verwendung der PUF 6 freigebbar oder einschränkbar sein, indem die Kommunikationsschnittstelle 9 freigegeben oder gesperrt wird. Beispielsweise kann die Kommunikationsschnittstelle 9 gesperrt werden. Gesperrt werden kann beispielsweise ein weiterer Funktionsblock (z.B. ein HF-Kommunikations-Funktionsblock eines RFID-Chips mit PUF-basierter Authentisierung, oder eine I2C-Schnittstelle), welche in der Schaltkreiseinheit integriert oder extern ist.

Gemäß einer weiteren bevorzugten Ausführungsform ist die Verwendung der PUF 6 mittels eines durch die PUF 6 bestimmten kryptographischen Parameters freigebbar oder einschränkbar, vorzugsweise indem durch einen Fuzzy Key Extractor ein kryptographischer Schlüssel ermittelbar ist. Beispielsweise kann das Ausgeben des Schlüssels gesperrt werden. Mit andern Worten kann damit in einem nachfolgenden Verarbeitungsschritt als beispielsweise bei der direkten Sperrung der externen Kommunikationsschnittstelle 9 der PUF-Zugriff mittels einer solchen Funktion gesperrt werden. So kann z.B. ein Fuzzy-Key-Extractor-Funktionsblock zur von PUF-Response-Werten abhängigen Ableitung eines kryptographischen Schlüssels, oder eine Schlüsselausgabe-Funktionsblock zur Bereitstellung eines kryptographischen Schlüssels gesperrt werden.

Gemäß einer weiteren bevorzugten Ausführungsform ermittelt die Prüfeinheit 5 im Rahmen des Vergleiches ein Übereinstimmungsmaß. Das Übereinstimmungsmaß wird mit einem Schwellwert verglichen. Falls das ermittelte Übereinstimmungsmaß den Schwellwert erreicht oder übertrifft, wird die Verwendung der PUF 6 freigegeben oder eingeschränkt. Selbstverständlich können auch bei geeigneter Wahl auch bei einem Unterschreiten des Schwellwertes die geeigneten Maßnahmen vorgenommen wer-

den, und je nach Ausführungsform die PUF freigegeben oder eingeschränkt werden. Ebenso kann der Schwellwert für mehrere Nutzungszwecke der PUF 6 konfigurierbar sein, und/oder es können unterschiedlichen Nutzungszwecken unterschiedliche Schwellwerte zugeordnet werden. Die Nutzung der PUF wird abhängig vom Vergleichsergebnis gegebenenfalls nur für manche Nutzungszwecke gesperrt, für andere jedoch freigegeben. Konkret könnten zwei kryptographische Schlüssel aus der PUF abgeleitet werden. Abhängig vom Vergleichsergebnis wird der Zugriff auf beide Schlüssel, auf nur den ersten Schlüssel (bzw. nur auf den zweiten Schlüssel), oder auf keinen Schlüssel freigegeben.

Gemäß weiteren bevorzugten Ausführungsformen kann die Prüfeinheit im Rahmen des Vergleiches überprüfen, ob die Response R1 mit der PUF-Response PR1 ausreichend übereinstimmt. Um die Aussagekraft des Vergleichs zu erhöhen, kann die Prüfeinheit aber im Rahmen des Vergleiches auch für mehrmalige Eingabe der Challenge Information C1 in die PUF 6 überprüfen, ob die dadurch durch die PUF 6 erzeugten PUF-Responses PRi ausreichend mit der Response R1 übereinstimmen. Ebenso kann die Prüfeinheit im Rahmen des Vergleiches für mehrere Challenge-Response-Paare CRi, welche jeweils eine Challenge-Information Ci und eine zu der Challenge- Information Ci zugeordnete Response-Information Ri umfassen, überprüfen, ob die aufgrund der Eingaben der Challenge Information Ci in die PUF 6 durch die PUF 6 erzeugten PUF-Responses PRi ausreichend mit den jeweiligen Responses Ri übereinstimmen.

Gemäß bevorzugten Ausführungsformen führt eine PUF-Baugruppe einen Selbsttest durch, bevor Zugriff auf die PUF-Funktionalität bereitgestellt wird (z.B. zur Authentisierung oder Schlüsselbestimmung). Dazu erfolgt mittels in dem Datenspeicher 7 gespeicherter Referenzdaten eine Selbstprüfung der PUF 6. Wenn diese erfolgreich ist, wird der Zugriff auf die PUF 6 freigegeben.

Figur 4 zeigt ein Flussdiagramm 20 für eine bevorzugte Ausführungsform des erfinderischen Verfahrens 20, welches durch die in Figur 3 dargestellte Schaltkreiseinheit durchführbar ist.

Das Verfahren 20 erlaubt das Durchführen eines Selbsttestes für die Schaltkreiseinheit 1. Mit dem Verfahrensschritt 21 wird das Verfahren 20 gestartet. Standardmässig ist der Zugriff auf die PUF 6 gesperrt, dargestellt durch Verfahrensschritt 22. Im Verfahrensschritt 23 erfasst die Prüfeinheit 5 Testdaten, beispielsweise das Challenge-Response-Paar CR1. Die Challenge-Information C1 des Challenge-Response-Paares CR1 wird dann in die PUF 6 eingegeben. Daraufhin liefert die PUF eine PUF-Response PR1. Die PUF-Response PR1 und die Response-Information R1 wird dann durch die Prüfeinheit 5 verglichen, dargestellt durch den Verfahrensschritt 24. In dem Verfahrensschritt 25 wird ein PUF-Konfidenzwert ermittelt. Beispielsweise lässt der Konfidenzwert eine Aussage darüber zu, wie gut die PUF-Response PR1 und die Response-Information R1 übereinstimmen. Ein hoher Konfidenzwert entspricht dabei einer guten Übereinstimmung. Übertrifft der Konfidenzwert einen Schwellwert, was im Verfahrensschritt 26 übeprüft wird, so wird im Verfahrensschritt 27 der Zugriff auf die PUF 6 freigegeben. Übertrifft der Konfidenzwert den Schwellwert jedoch nicht, so wird im Rahmen des Verfahrensschrittes 28 der Zugriff auf die PUF 6 nicht freigegeben. Abhängig vom Ergebnis des Vergleichs wird somit also eine Verwendung der PUF 6 freigegeben oder eingeschränkt. Verfahrensschritt 29 stellt das Ende des Verfahrens dar.

Gemäß einer bevorzugten Ausührungsform der Erfindung wird eine Funktionsprüfung für eine PUF vorgeschlagen. Diese kann in eine PUF-Einheit als Selbsttest integriert sein oder ggf. auch separat vorliegen. Vor einer Verwendungsfreigabe der PUF bzw. einer Security-Funktionalität des Gerätes, in das die PUF integriert ist, erfolgt die Funktionsprüfung der PUF.

Die Prüfung kann zu unterschiedlichen Zeitpunkten bzw. Ereignissen erfolgen:

- Fertigung
- Inbetriebnahme
- Booten / nach Strom anlegen
- regelmäßig im Betrieb wiederkehrend,… ; z.B. in regelmäßigen Zeitintervallen, oder interleaved mit Berechnung externer, „scharf" genutzter Challenges (int, ext, int, ext, …).

Die Prüfung kann eine der mehreren der folgenden Prüfungen umfassen:

- Ermitteln von statistischen Kenngrößen von mehrerer Antworten mit gleichen Challenge-Werten (z.B. Hamming-Distanz: Minimum/Maximum,/Mittelwert/Varianz/Standardabweichung der Hamming-Distanz). Diese müssen in einem bestimmten Bereich liegen.
- Prüfen mittels bekannten Test Challenge-/Response-Paaren: Fehlerabweichung (Hamming-Distanz der Response einer Challenge mit der bekannten Response-Werten ermitteln und mit Schwellwert vergleichen. Der Schwellwert wird sinnvollerweise „enger" (vorsichtiger) gesetzt als für einen operativen Betrieb erforderlich. Falls aus einer PUF z.B. ein Schlüssel mittels einer Key Extractor Funktion bestimmt wird, wobei z.B. bis zu 20 Bitfehler korrigierbar sind, so erfolgt zuerst ein Test der PUF (mit anderen Challenge-Test-Werten), wobei maximal 10 oder 15 Bitfehler auftreten dürfen, um eine weitere Nutzung der PUF für die Schlüsselextraktion zuzulassen. Alternativ kann auch aus PUF mit ersten Satz von Challenge-Werten ein erster Key extrahiert und mittels gespeicherter Referenzinformation geprüft werden. Einen zweiter (scharfer) Key wird nur extrahiert bzw. nur verwendet, wenn der erste Key als gültig erkannt ist. Auch hier kann beim ersten Key eine „zurückhaltendere" (weniger Fehler korrigierende) Fehlerkorrektur angewandt werden im Vergleich zur Extraktion eines „scharfen" Schlüssels.

Patentansprüche

1. Schaltkreiseinheit (1) umfassend eine im Folgenden PUF (6) genannte Physical Unclonable Function (6), eine Prüfeinheit (5) und einen Informationsspeicher (7) zum Speichern mindestens eines Challenge-Response-Paares (CR1);
wobei das Challenge-Response-Paar (CR1) eine Challenge-Information (C1) und eine dazu gehörige Response-Information (R1) umfasst; und
wobei die Prüfeinheit (5) ausgestaltet und/oder adaptiert ist, eine Eingabe der Challenge-Information (C1) in die PUF (6) zu veranlassen, und eine darauf durch die PUF (6) erzeugte PUF-Response (PR1) und die Response-Information (R1) für einen Vergleich zu verwenden und abhängig vom Ergebnis des Vergleichs eine Verwendung der PUF (6) freizugeben oder einzuschränken.

2. Schaltkreiseinheit (1) nach Anspruch 1, wobei die Schaltkreiseinheit (1) ein integrierter Schaltkreis (1) ist.

3. Schaltkreiseinheit (1) nach einem der vorhergehenden Ansprüche, umfassend eine Schnittstelle (9) durch welche ein Zugriff von extern auf die PUF (6) vornehmbar ist.

4. Schaltkreiseinheit (1) nach einem der vorhergehenden Ansprüche, wobei die Verwendung der PUF (6) freigebbar oder einschränkbar ist, indem der Zugriff auf die PUF (6) direkt freigegeben oder gesperrt wird.

5. Schaltkreiseinheit (1) nach einem der vorhergehenden Ansprüche, wobei die Verwendung der PUF (6) freigebbar oder einschränkbar ist, indem die Schnittstelle (9) freigegeben oder gesperrt wird.

6. Schaltkreiseinheit (1) nach einem der vorhergehenden Ansprüche, wobei die Verwendung der PUF (6) mittels eines durch die PUF (6) bestimmten kryptographischen Parameters freigebbar oder einschränkbar ist, vorzugwseise indem durch einen

Fuzzy Key Extractor ein kryptographischer Schlüssel ermittelbar ist, wobei das Ausgeben des Schlüssels gesperrt werden kann.

7. Schaltkreiseinheit (1) nach einem der vorhergehenden Ansprüche, wobei die Prüfeinheit (5) ausgestaltet und/oder adaptiert ist, im Rahmen des Vergleiches ein Übereinstimmungsmaß zu ermitteln, welches mit einem Schwellwert verglichen wird, und die Verwendung der PUF (6) freigegeben oder eingeschränkt wird, falls das ermittelte Übereinstimmungsmaß den Schwellwert erreicht, übertrifft oder unterschreitet.

8. Schaltkreiseinheit (1) nach Anspruch 7, wobei der Schwellwert für mehrere Nutzungszwecke der PUF (6) konfigurierbar ist, wobei unterschiedlichen Nutzungszwecken unterschiedliche Schwellwerte zuordenbar sind.

9. Schaltkreiseinheit (1) nach einem der vorhergehenden Ansprüche, wobei die Prüfeinheit (5) ausgestaltet und/oder adaptiert ist, im Rahmen des Vergleiches zu überprüfen, ob:
a) die Response (R1) mit der PUF-Response (PR1) ausreichend übereinstimmt; oder
b) für mehrmalige Eingabe der Challenge Information (C1) in die PUF (6) die dadurch durch die PUF (6) erzeugten PUF-Responses (PRi) ausreichend mit der Response (R1) übereinstimmen; oder
c) für mehrere Challenge-Response-Paare (CRi), welche jeweils eine Challenge-Information (Ci) und eine zu der Challenge-Information (Ci) zugeordnete Response-Information (Ri) umfassen, die aufgrund der Eingaben der Challenge Information (Ci) in die PUF (6) durch die PUF (6) erzeugten PUF-Responses (PRi) ausreichend mit den jeweiligen Responses (Ri) übereinstimmen.

10. Verfahren zum Durchführen eines Selbstestes für eine Schaltkreiseinheit (1) welche eine im Folgenden PUF (6) genannte Physical Unclonable Function (6), eine Prüfeinheit (5) und einen Informationsspeicher (7) zum Speichern mindestens

eines Challenge-Response-Paares (CR1) umfasst, wobei das Challenge-Response-Paar (CR1) eine Challenge-Information (C1) und eine dazu gehörige Response-Information (R1) umfasst, das Verfahren umfassend die Verfahrensschritte:

Eingeben der Challenge-Information (C1) in die PUF (6);

Verwenden einer darauf durch die PUF (6) erzeugten PUF-Response (PR1) und der Response-Information (R1) für einen durch die Prüfeinheit 5 durchgeführten Vergleich, wobei abhängig vom Ergebnis des Vergleichs eine Verwendung der PUF (6) freigegeben oder eingeschränkt wird.

11. Verfahren nach Anspruch 10, wobei die Schaltkreiseinheit (1) ein integrierter Schaltkreis (1) ist.

12. Verfahren nach Anspruch 10 oder 11, wobei die Schaltkreiseinheit eine Schnittstelle (9) umfasst, durch welche aufgrund des Vergleichs ein Zugriff von extern auf die PUF 6 vorgenommen wird.

13. Verfahren nach einem der Ansprüche 10 bis 12, wobei die Verwendung der PUF (6) wobei die Verwendung der PUF direkt freigegeben oder gesperrt wird.

14. Verfahren nach einem der Ansprüche 10 bis 13, wobei die Verwendung der PUF (6) freigegeben oder eingeschränkt wird, indem die Schnittstelle (9) freigegeben oder eingeschränkt wird.

15. Verfahren nach einem der Ansprüche 10 bis 14, wobei die Verwendung der PUF (6) mittels eines durch die PUF (6) bestimmten kryptographischen Parameters freigegeben oder eingeschränkt wird, vorzugwseise indem durch einen Fuzzy Key Extractor ein kryptographischer Schlüssel ermittelt wird, wobei das Ausgeben des Schlüssels gesperrt werden kann und so die Verwendung der PUF (6) eingeschränkt wird.

16. Verfahren nach einem der Ansprüche 10 bis 15, wobei im Rahmen des Vergleiches ein Übereinstimmungsmaß ermittelt

wird, welches mit einem Schwellwert verglichen wird, und die Verwendung der PUF (6) freigegeben oder eingeschränkt wird, falls das ermittelte Übereinstimmungsmaß den Schwellwert erreicht, übertrifft oder unterschreitet.

17. Verfahren nach einem der Ansprüche 10 bis 16, wobei der Schwellwert für mehrere Nutzungszwecke der PUF (6) konfiguriert wird, wobei unterschiedlichen Nutzungszwecken unterschiedliche Schwellwerte zuordenbar sind.

18. Verfahren nach einem der Ansprüche 10 bis 17, wobei im Rahmen des Vergleiches überprüft wird, ob:
a) die Response (R1) mit der PUF-Response (PR1) ausreichend übereinstimmt; oder
b) für mehrmalige Eingabe der Challenge Information (C1) in die PUF (6) die dadurch durch die PUF (6) erzeugten PUF-Responses (PRi) ausreichend mit der Response (R1) übereinstimmen; oder
c) für mehrere Challenge-Response-Paare (CRi), welche jeweils eine Challenge-Information (Ci) und eine zu der Challenge-Information (Ci) zugeordnete Response-Information (Ri) umfassen, die aufgrund der Eingaben der Challenge Information (Ci) in die PUF (6) durch die PUF (6) erzeugten PUF-Responses (PRi) ausreichend mit den jeweiligen Responses (Ri) übereinstimmen.

FIG 1

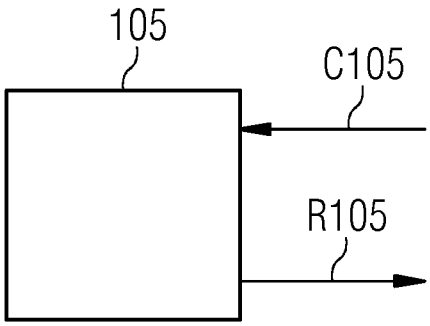


FIG 2

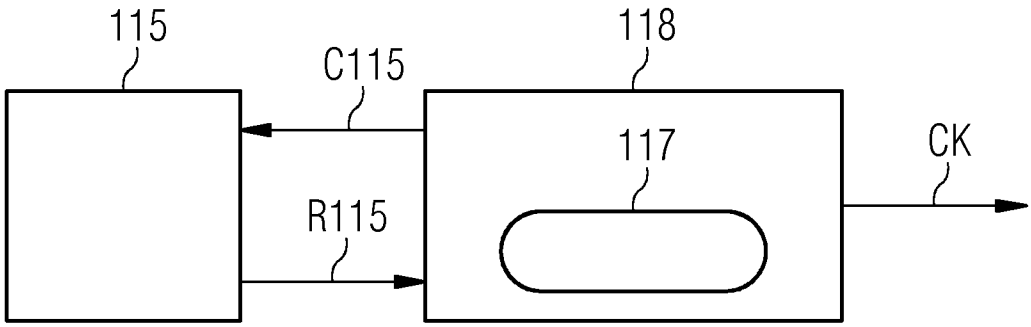


FIG 3

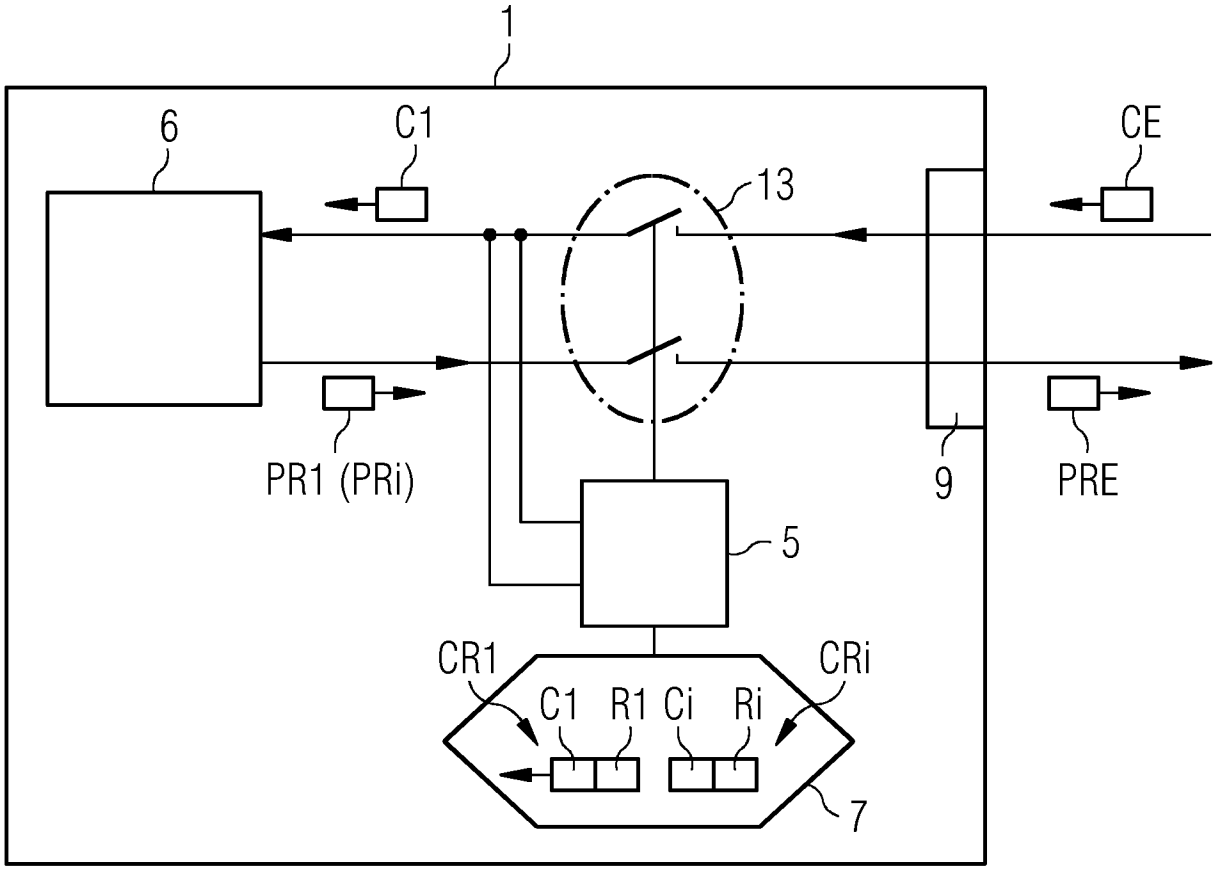
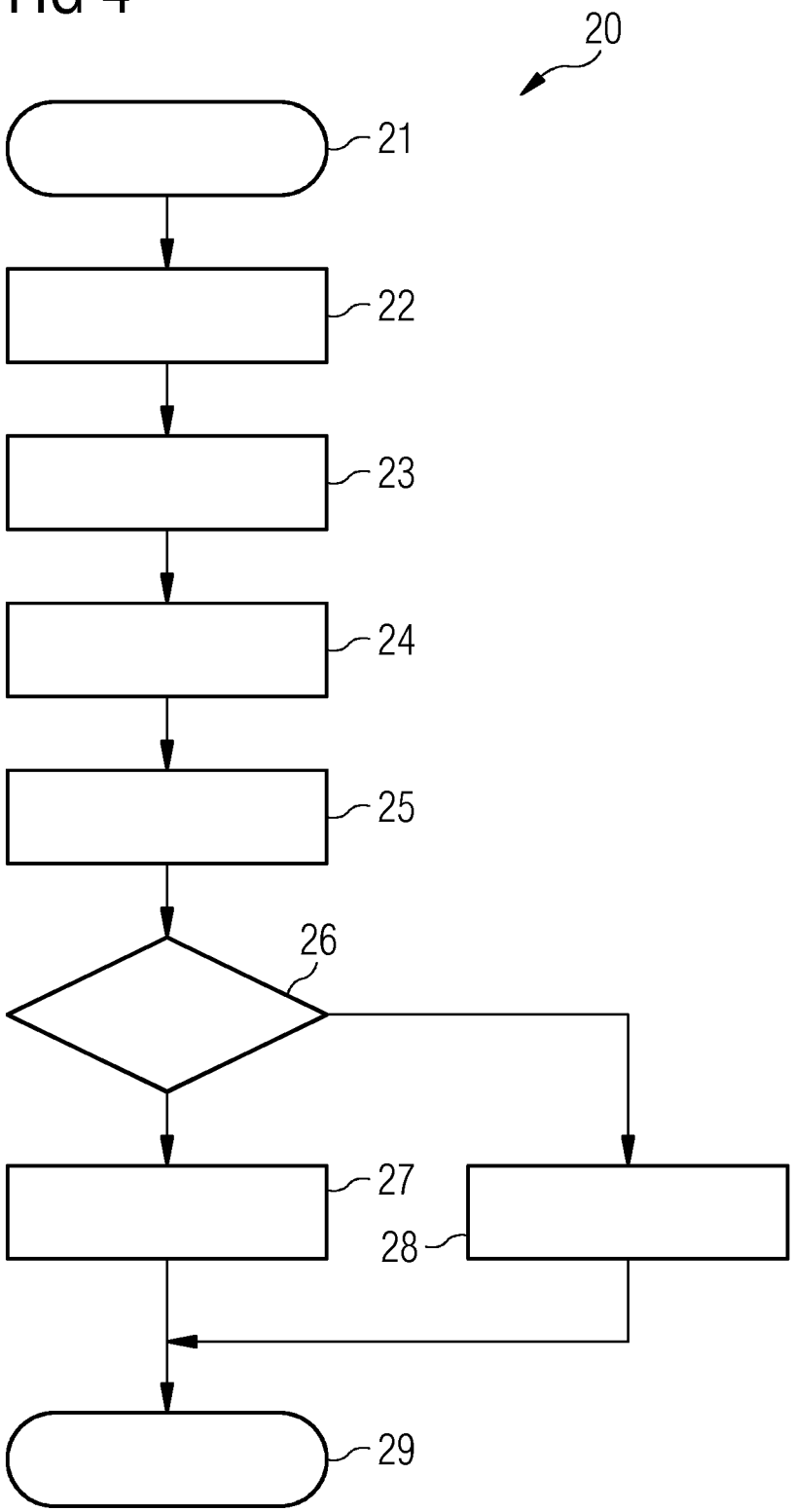


FIG 4



INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2013/066653

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/57 G01R31/3187 G06F11/27 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)
G06F G01R 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 2011/055649 A1 (KOUSHANFAR FARINAZ [US] ET AL) 3 March 2011 (2011-03-03) the whole document	1-18
A	AA KORIÄ B ET AL: "Robust Key Extraction from Physical Uncloneable Functions", 19 May 2005 (2005-05-19), APPLIED CRYPTOGRAPHY AND NETWORK SECURITY; [LECTURE NOTES IN COMPUTER SCIENCE;;LNCS], SPRINGER-VERLAG, BERLIN/HEIDELBERG, PAGE(S) 407 - 422, XP019010616, ISBN: 978-3-540-26223-7 cited in the application the whole document	1-18

☐ Further documents are listed in the continuation of Box C.

☒ 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
8 January 2014	17/01/2014

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	Mäenpää, Jari

1

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2013/066653

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2011055649 A1	03-03-2011	NONE	

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP2013/066653

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
INV. G06F21/57 G01R31/3187 G06F11/27 H04L9/32
ADD.

Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
G06F G01R H04L

Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 2011/055649 A1 (KOUSHANFAR FARINAZ [US] ET AL) 3. März 2011 (2011-03-03) das ganze Dokument	1-18
A	AA KORIÄ B ET AL: "Robust Key Extraction from Physical Uncloneable Functions", 19. Mai 2005 (2005-05-19), APPLIED CRYPTOGRAPHY AND NETWORK SECURITY; [LECTURE NOTES IN COMPUTER SCIENCE;;LNCS], SPRINGER-VERLAG, BERLIN/HEIDELBERG, PAGE(S) 407 - 422, XP019010616, ISBN: 978-3-540-26223-7 in der Anmeldung erwähnt das ganze Dokument	1-18

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen ☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" frühere Anmeldung oder Patent, die bzw. das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
8. Januar 2014	17/01/2014

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Mäenpää, Jari

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP2013/066653

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 2011055649 A1	03-03-2011	KEINE	