(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
5. Juli 2001 (05.07.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/48974 A1

(51) Internationale Patentklassifikation[7]: H04L 9/30, G06F 7/72

(21) Internationales Aktenzeichen: PCT/EP00/13031

(22) Internationales Anmeldedatum:
20. Dezember 2000 (20.12.2000)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
199 63 408.4 28. Dezember 1999 (28.12.1999) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **GIESECKE & DEVRIENT GMBH** [DE/DE]; Prinzregentenstrasse 159, 81677 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **DREXLER, Hermann** [DE/DE]; Oberländerstrasse 5a, 81371 München (DE). **VATER, Harald** [DE/DE]; An den Schulgärten 23, 35398 Giessen (DE).

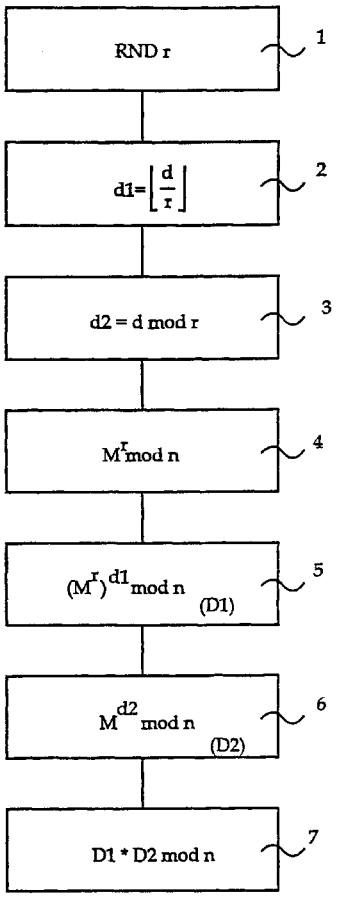
(74) Anwalt: **KLUNKER, SCHMITT-NILSON, HIRSCH**; Winzererstr. 106, 80797 München (DE).

(81) Bestimmungsstaaten *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

[Fortsetzung auf der nächsten Seite]

(54) Title: PORTABLE DATA CARRIER PROVIDED WITH ACCESS PROTECTION BY DIVIDING UP CODES

(54) Bezeichnung: TRAGBARER DATENTRÄGER MIT ZUGRIFFSSCHUTZ DURCH SCHLÜSSELTEILUNG



(57) **Abstract:** The invention relates to a data carrier comprising a semiconductor chip provided with at least one memory in which an operating program is stored. Said operating program contains a number of instructions, whereby each instruction is elicited by signals that can be detected outside of the semiconductor chip. The aim of the invention is to protect secret data, which is provided in the chip of the data carrier, from "Differential Power Analysis" (DPA) or Higher Order DPA. To this end, the invention provides that in order to carry out security-relevant operations in the semiconductor chip, the data carrier is designed for dividing up secret data, which is stored or generated by the same, into at least three data parts, whereby an arithmetic unit for calculating a random number and for dividing the random number is contained therein, whereby the first data part is the integer result of the division, the second part is the remainder of the division, and the third part is the random number itself.

(57) **Zusammenfassung:** Die Erfindung betrifft einen Datenträger mit einem Halbleiterchip der wenigstens einen Speicher aufweist, in dem ein Betriebsprogramm abgelegt ist, das mehrere Befehle beinhaltet, wobei jeder Befehl von ausserhalb des Halbleiterchips detektierbare Signale hervorruft. Es ist Aufgabe der Erfindung, geheime Daten, die im Chip des Datenträgers vorhanden sind, vor "Differential Power Analysis" (DPA) bzw. Higher Order DPA zu schützen. Gemäss der Erfindung ist der Datenträger ausgelegt, um zur Durchführung sicherheitsrelevanter Operationen im Halbleiterchip abgelegte oder von diesem generierte geheime Daten in mindestens drei Datenteile aufzuteilen, wobei eine Recheneinheit zum Berechnen einer Zufallszahl und zur Teilung der Zufallszahl enthalten ist, wobei der erste Datenteil das ganzzahlige Ergebnis der Teilung ist, der zweite Teil der Rest der Teilung und der dritte Teil die Zufallszahl selbst ist.

WO 01/48974 A1

(84) **Bestimmungsstaaten** *(regional)*: ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *Mit internationalem Recherchenbericht.*

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.