



(11) **EP 1 668 515 B8**

(12) **KORRIGIERTE EUROPÄISCHE PATENTSCHRIFT**

(15) Korrekturinformation:
Korrigierte Fassung Nr. 1 (W1 B1)
Korrekturen, siehe
Bibliographie INID code(s) 84

(51) Int Cl.:
G06F 12/14 ^(2006.01)

(86) Internationale Anmeldenummer:
PCT/EP2004/009054

(48) Corrigendum ausgegeben am:
21.03.2012 Patentblatt 2012/12

(87) Internationale Veröffentlichungsnummer:
WO 2005/043396 (12.05.2005 Gazette 2005/19)

(45) Veröffentlichungstag und Bekanntmachung des
Hinweises auf die Patenterteilung:
05.10.2011 Patentblatt 2011/40

(21) Anmeldenummer: **04741411.5**

(22) Anmeldetag: **12.08.2004**

(54) **WORTINDIVIDUELLE SCHLÜSSELERZEUGUNG**

WORD-INDIVIDUAL KEY GENERATION

PRODUCTION D'UNE CLE INDIVIDUELLE A CHAQUE MOT

(84) Benannte Vertragsstaaten:
DE FR

WO-A-00/55736 GB-A- 2 264 373
US-A- 4 319 079 US-A- 5 915 025
US-A1- 2003 105 967 US-B1- 6 345 359

(30) Priorität: **30.09.2003 DE 10345454**

(43) Veröffentlichungstag der Anmeldung:
14.06.2006 Patentblatt 2006/24

(73) Patentinhaber: **Infineon Technologies AG**
85579 Neubiberg (DE)

(72) Erfinder:
• **ELBE, Astrid**
81243 München (DE)
• **GAMMEL, Berndt**
85570 Markt Schwaben (DE)
• **GÖTTFERT, Rainer**
82024 Taufkirchen (DE)
• **SONNEKALB, Steffen**
82024 Taufkirchen (DE)

(74) Vertreter: **Schenk, Markus et al**
Schoppe, Zimmermann, Stöckeler & Zinkler
Patentanwälte
Postfach 246
82043 Pullach bei München (DE)

(56) Entgegenhaltungen:

- **ITOH K ET AL: "DPA countermeasure based on the "masking method"" INFORMATION SECURITY AND CRYPTOLOGY - ICISC 2001. 4TH INTERNATIONAL CONFERENCE. PROCEEDINGS (LECTURE NOTES IN COMPUTER SCIENCE VOL.2288) SPRINGER-VERLAG BERLIN, GERMANY, Dezember 2001 (2001-12), Seiten 440-456, XP002322028 ISBN: 3-540-43319-8**
- **LABBE A ET AL: "DES-SRAM IP-core: a SRAM embedding DES feature" SOC CONFERENCE, 2003. PROCEEDINGS. IEEE INTERNATIONAL [SYSTEMS-ON-CHIP] 17-20 SEPT. 2003, PISCATAWAY, NJ, USA,IEEE, 17. September 2003 (2003-09-17), Seiten 11-14, XP010665813 ISBN: 0-7803-8182-3**
- **PANATO A ET AL: "A low device occupation IP to implement Rijndael algorithm" DESIGN, AUTOMATION AND TEST IN EUROPE CONFERENCE AND EXHIBITION, 2003 MUNICH, GERMANY 3-7 MARCH 2003, LOS ALAMITOS, CA, USA,IEEE COMPUT. SOC, US, 3. März 2003 (2003-03-03), Seiten 20-25, XP010674193 ISBN: 0-7695-1870-2**

Anmerkung: Innerhalb von neun Monaten nach Bekanntmachung des Hinweises auf die Erteilung des europäischen Patents im Europäischen Patentblatt kann jedermann nach Maßgabe der Ausführungsordnung beim Europäischen Patentamt gegen dieses Patent Einspruch einlegen. Der Einspruch gilt erst als eingelegt, wenn die Einspruchsgebühr entrichtet worden ist. (Art. 99(1) Europäisches Patentübereinkommen).

EP 1 668 515 B8