(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 3 742 319 B8**

(12) **KORRIGIERTE EUROPÄISCHE PATENTSCHRIFT**

(15) Korrekturinformation:
Korrigierte Fassung Nr. 1 (W1 B1)
Korrekturen, siehe
Bibliographie INID code(s) 73

(48) Corrigendum ausgegeben am:
08.11.2023 Patentblatt 2023/45

(45) Veröffentlichungstag und Bekanntmachung des Hinweises auf die Patenterteilung:
20.09.2023 Patentblatt 2023/38

(21) Anmeldenummer: **20020237.2**

(22) Anmeldetag: **19.05.2020**

(51) Internationale Patentklassifikation (IPC):
G06F 21/60 *(2013.01)* ***G06F 21/64*** *(2013.01)*
H04L 9/32 *(2006.01)*

(52) Gemeinsame Patentklassifikation (CPC):
H04L 9/3242; G06F 21/60; G06F 21/606; G06F 21/64; H04L 2209/72

(54) **SEITENKANALSICHERE IMPLEMENTIERUNG**

SIDE CHANNEL SECURE IMPLEMENTATION

MISE EN OEUVRE SÉCURISÉE DU CANAL LATÉRAL

(84) Benannte Vertragsstaaten:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

(30) Priorität: **24.05.2019 DE 102019003673**

(43) Veröffentlichungstag der Anmeldung:
25.11.2020 Patentblatt 2020/48

(73) Patentinhaber: **Giesecke+Devrient ePayments GmbH**
81677 München (DE)

(72) Erfinder:
- **Stocker, Thomas**
  81739 München (DE)
- **Hirschinger, Jürgen**
  85375 Neufahrn (DE)

(74) Vertreter: **Giesecke + Devrient IP**
Prinzregentenstraße 161
81677 München (DE)

(56) Entgegenhaltungen:
EP-A1- 3 376 426
WO-A1-2019/081919
US-A1- 2007 245 147
US-A1- 2018 294 968

- **KUROKAWA TAKASHI ET AL: "Can We Securely Use CBC Mode in TLS1.0?", 19. November 2015 (2015-11-19), 12TH EUROPEAN CONFERENCE ON COMPUTER VISION, ECCV 2012; [LECTURE NOTES IN COMPUTER SCIENCE], SPRINGER BERLIN HEIDELBERG, BERLIN GERMANY, PAGE(S) 151 - 160, XP047523950, ISSN: 0302-9743 ISBN: 978-3-319-23527-1 [gefunden am 2015-11-19] * Abbildung 1 ***

EP 3 742 319 B8