UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/805,431	07/21/2015	Hugues de Perthuis	81639041US03	8485

65913 7590 01/28/2019

Intellectual Property and Licensing
NXP B.V.
411 East Plumeria Drive, MS41
SAN JOSE, CA 95134

EXAMINER	
TABOR, AMARE F	

ART UNIT	PAPER NUMBER
2434	

NOTIFICATION DATE	DELIVERY MODE
01/28/2019	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ip.department.us@nxp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte HUGUES DE PERTHUIS

Appeal 2018-005121
Application 14/805,431
Technology Center 2400

Before ELENI MANTIS MERCADER, CARL W. WHITEHEAD JR., and NORMAN H. BEAMER, *Administrative Patent Judges*.

MANTIS MERCADER, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

Appellant[1] appeals under 35 U.S.C. § 134(a) from the Examiner's final rejection of claims 1–17, which constitute all the pending claims in this application. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm.

---

[1] Appellant does not identify the real party in interest; however, the real party in interest appears to be NXP B.V. *See* App. Br. 13.

THE INVENTION

Appellant's claimed invention is directed to "securely encrypting and decrypting data" within the memory of a device in order to "prevent[] successful decryption in the event of execution of modified or malicious code that alters the data" stored in the memory (Abstract).

Independent claim 1, reproduced below, is representative of the subject matter on appeal:

> 1. A method of encrypting data stored within a non-transitory computer readable memory of a device, the method comprising:
>
> providing a key;
>
> encrypting the data stored in the non-transitory computer readable memory using the key;
>
> generating an authentication code based on all contents of a defined source code area stored in the non-transitory computer readable memory;
>
> wrapping the key using the authentication code to generate a wrapped key; and
>
> storing the wrapped key in the non-transitory computer readable memory, wherein validity of the wrapped key is linked to authenticity of the data stored in the non-transitory computer readable memory.

App. Br. 14 (Claims Appendix).

REFERENCES

The prior art relied upon by the Examiner in rejecting the claims on appeal is the following:

Cheng	US 2005/0036617 A1	Feb. 17, 2005
Alghathbar	US 2011/0296193 A1	Dec. 1, 2011
Sussland	US 8,213,620 B1	July 3, 2012
Campello de Souza	US 8,312,269 B2	Nov. 13, 2012
Harwood	US 8,498,417 B1	July 30, 2013
Wang	US 2013/0311781 A1	Nov. 21, 2013

REJECTIONS

The Examiner made the following rejections:

Claims 1–6, 10–13, 16, and 17 stand rejected under 35 U.S.C. § 103 as unpatentable over Campello de Souza, in view of Harwood and/or Sussland, and further in view of Alghathbar. Final Act. 2.

Claims 7–9 stand rejected under 35 U.S.C. § 103 as unpatentable over Campello de Souza, in view of Harwood and/or Sussland, and further in view of Alghathbar and Wang. Final Act. 9.

Claims 14 and 15 stand rejected under 35 U.S.C. § 103 as unpatentable over Campello de Souza, in view of Harwood and/or Sussland, and further in view of Alghathbar and Cheng. Final Act. 10.[2]

ISSUE

The pivotal issue is whether the Examiner erred in finding Alghathbar teaches or suggests the limitation of "generating an authentication code based on all contents of a defined source code area stored in the non-

[2] The heading of the rejection incorrectly omits the reference Alghathbar, whereas the body of the rejection refers to Alghathbar. *See* Final Act. 11.

transitory computer readable memory," as recited in independent claim 1, and similarly recited in independent claims 11 and 14.

ANALYSIS

We adopt the Examiner's findings in the Answer and Final Office Action and we add the following primarily for emphasis. We note that if Appellant failed to present arguments on a particular rejection, we will not unilaterally review those uncontested aspects of the rejection. *See Ex parte Frye*, 94 USPQ2d 1072, 1075 (BPAI 2010) (precedential); *Hyatt v. Dudas*, 551 F.3d 1307, 1313–14 (Fed. Cir. 2008) (the Board may treat arguments Appellant failed to make for a given ground of rejection as waived).

Appellant argues "Alghathbar fails to generate an authentication code based on **all contents** of a defined source code area stored in the non-transitory computer readable memory" because "Alghathbar discloses that a 'hash function is built based upon respective **portions** of the secret key and a language interpreter'" (Reply Br. 2, citing Alghathbar ¶ 2, emphasis in original). Appellant further contends that "because Alghathbar's 128-bit hash code of X involves use of secret key K to permute the order of message X," it follows that "Alghathbar's technique necessarily requires the use of input secret key K" and is thus different from "generating an authentication code based on **all contents** of a defined source code area" (Reply Br. 3, citing Fig. 3 item 310 and ¶ 39, emphasis in original).

We are not persuaded by Appellant's arguments. With respect to the claimed "based on all contents of a defined source code area," the Examiner finds that "Alghathbar meets the claimed limitation because it teaches using 'all contents' (of message X) as a source code to generate/compute an

authentication code" (Ans. 14, citing Alghathbar Figs. 2 item 214, Figs. 3 and 5, ¶¶ 18, 28). Here, the cited portion of Alghathbar explicitly states "[t]he input message will be used as a source code . . . to generate a 128-bit hash code of X" (Alghathbar ¶ 28).

Further, with respect to Appellant's argument that "Alghathbar's technique necessarily requires the use of input secret key K" (Reply Br. 3) to generate the authentication code whereas Appellant's claimed method does not require a secret key, Appellant's claim explicitly recites "based on"—not "based solely on" or "based only on" or another variant—and additionally recites the preamble transition "comprising," which allows for additional elements. Thus, the claimed method encompasses Alghathbar's use of a secret key.

Accordingly, we affirm the Examiner's rejection of independent claim 1, and independent claims 11 and 14 not separately argued with particularity, as well as dependent claims 2–10, 12, 13, and 15–17 not separately argued with particularity. *See* App. Br. 7–12.

CONCLUSION

The Examiner did not err in finding Alghathbar teaches or suggests the limitation of "generating an authentication code based on all contents of a defined source code area stored in the non-transitory computer readable memory," as recited in independent claim 1, and similarly recited in independent claims 11 and 14.

DECISION

The Examiner's decision rejecting claims 1–17 under 35 U.S.C. § 103 is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(l)(iv).

AFFIRMED