



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.
12/434,260	05/01/2009	Douglas Wayne WALKER	RF-514 (50704)	1785
74701	7590	12/02/2016	EXAMINER	
ADDMG - Harris 255 S ORANGE AVENUE SUITE 1401 ORLANDO, FL 32801			HOLDER, BRADLEY W	
			ART UNIT	PAPER NUMBER
			2439	
			NOTIFICATION DATE	DELIVERY MODE
			12/02/2016	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):

creganoa@addmg.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte DOUGLAS WAYNE WALKER and
CHRISTOPHER DAVID MACKEY

Appeal 2014-008166
Application 12/434,260¹
Technology Center 2400

Before ELENI MANTIS MERCADER, JEFFREY A. STEPHENS, and
SCOTT E. BAIN, *Administrative Patent Judges*.

BAIN, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellants appeal under 35 U.S.C. § 134(a) from the Examiner's Non-Final Rejection of claims 1–3, 5, 7–17, and 19–23, which constitute all claims pending in the application. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm.

¹ Appellants identify Harris Corporation as the real party in interest. App. Br. 2.

STATEMENT OF THE CASE

The claimed invention relates to a secure hashing device configured to process a message using a given secure hash algorithm (“SHA”) among different SHA variants. Abstract; Spec. ¶ 8. Claims 1, 12, and 19 are independent. Claims 1 and 12 are illustrative of the invention and the subject matter of the appeal, and read as follows:

1. A monolithic integrated circuit (IC) secure hashing device comprising:

a plurality of registers comprising a mode register configured to store a mode of operation value; and

a processor integrated with said plurality of registers and configured to

receive a message,

select a given secure hash algorithm (SHA) variant based upon the mode of operation value,

process the message using the given SHA variant from among a plurality of different SHA variants, the plurality of different SHA variants being based upon corresponding different block sizes of bits, and

cooperate with said plurality of registers for selecting the different block sizes of bits for the plurality of different SHA variants and for controlling SHA processing of the message.

12. A monolithic integrated circuit (IC) secure hashing device comprising:

a plurality of registers comprising a mode register configured to store a mode of operation value, and a status register configured to store a hash operation status value; and

a processor integrated with said plurality of registers and configured to

receive a message,

provide a wrapper file interface for external preprocessing of the message,

select a given secure hash algorithm-2 (SHA-2) variant based upon the mode of operation value,

process the message using the given SHA-2 variant from among a plurality of different SHA-2 variants, the plurality of different SHA-2 variants being based upon corresponding different block sizes of bits,

update the hash operation status value based upon the processing of the message, and

cooperate with said plurality of registers for selecting the different block sizes of bits for the plurality of different SHA variants and for controlling SHA processing of the message.

App. Br. 17, 19 (Claims App'x) (emphasis added).

THE REJECTIONS ON APPEAL

Claim 12 stands rejected under pre-AIA 35 U.S.C. § 112, first paragraph as failing to comply with the written description requirement. Non-Final Act. 5–6.

Claim 12 stands rejected under pre-AIA 35 U.S.C. § 112, second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor regards as the invention. *Id.* at 6–7.

Claims 1–3, 7, 8, 10, 11, 19–21, and 23 stand rejected under pre-AIA 35 U.S.C. § 103(a) as being unpatentable over Sklavos et al., *Implementation of the SHA-2 Hash Family Standard Using FPGAs*, 31 THE J. OF SUPERCOMPUTING 227–48 (2005) (“Sklavos”), Horanzy (US 2004/0093488 A1; May 13, 2004), and Crispin et al. (US 2005/0089160 A1; Apr. 28, 2005) (“Crispin”). *Id.* at 8–12.

Claims 12–14, 16, and 17 stand rejected under pre-AIA 35 U.S.C. § 103(a) as being unpatentable over Sklavos, Crispin, and Wheeler et al. (US 2005/0132226 A1; June 16, 2005) (“Wheeler”). *Id.* at 12–15.

Claims 5 and 22 stand rejected under pre-AIA 35 U.S.C. § 103(a) as being unpatentable over Sklavos, Horanzy, Crispin, and Vanstone et al. (US 2007/0076866 A1; Apr. 5, 2007) (“Vanstone”). *Id.* at 15–16.

Claim 9 stands rejected under pre-AIA 35 U.S.C. § 103(a) as being unpatentable over Sklavos, Horanzy, Crispin, and Childs et al. (US 5,623,545; Apr. 22, 1997) (“Childs”). *Id.* at 16–17.

Claim 15 stands rejected under pre-AIA 35 U.S.C. § 103(a) as being unpatentable over Sklavos, Wheeler, Crispin, and Vanstone. *Id.* at 17.

ANALYSIS

We have reviewed the Examiner’s rejections in light of Appellants’ arguments presented in this appeal. Arguments which Appellants could have made but did not make in the Briefs are deemed to be waived. *See* 37 C.F.R. § 41.37(c)(1)(iv). On the record before us, we are not persuaded the Examiner erred. We adopt as our own the findings and reasons set forth in the rejections from which the appeal is taken and in the Examiner’s Answer, and provide the following for highlighting and emphasis.

35 U.S.C. § 112, First Paragraph Rejection

Appellants argue the Examiner erred in finding the Specification does not adequately describe “provid[ing] a wrapper file interface for external pre-processing of the message,” as recited in claim 12. App. Br. 5.

Appellants contend the limitation is described in the Specification at paragraphs 31 to 34, as well as Figure 3. *Id.* at 5–6. We disagree.

The disputed limitations were added to claim 12 during prosecution. *See* Spec. 17 (claim 12 as originally filed). As the Examiner finds, Ans. 2–3, the term “wrapper file interface” does not appear in the Specification. Although the Specification states, “[t]he configurable SHA core . . . will reside within a wrapper file,” Spec. ¶ 34, it does not describe a wrapper file *interface*, nor is there any discussion connecting a wrapper file (interface) to “external pre-processing of [a] message,” as recited in the claim. Ans. 2–3. The Specification’s only mention of “pre-processing” is that the SHA core “leaves the preprocessing stage to software based approaches.” Spec. ¶¶ 32–33. Stating that the preprocessing is done in software, however, does not disclose the claim limitation reciting a *wrapper file interface* for *external* preprocessing of the message.

Appellants’ citation to Figure 3, App. Br. 5, also does not persuade us the Examiner erred. Figure 3 is reproduced below.

Core” (no corresponding number), and an area labeled “Bus Interface Wrapper” (also with no corresponding number.” Again, there is no mention of any “wrapper file interface” in Figure 3. Although the figure illustrates “bus *interface* logic” and “bus *interface wrapper*,” it is unclear from Appellants’ argument which of these elements is alleged to be the claimed “wrapper file interface,” and neither is described as such. Moreover, neither element is described as being “for external pre-processing of the message,” as claim 12 recites. Also, as the Examiner finds, it is unclear from Figure 3 what relationship the “bus interface wrapper” (which is not numbered) has to any other element, and that term is not even mentioned in the Specification. *See* Ans. 2–3.

Accordingly, we sustain the Examiner’s rejection of claim 12 under pre-AIA 35 U.S.C. § 112, first paragraph as failing to satisfy the written description requirement.

35 U.S.C. § 112, Second Paragraph Rejection

The Examiner rejects claim 12 as indefinite because, the Examiner finds, the limitation “providing a wrapper file interface for *external* pre-processing of the message” is ambiguous. Non-Final Act. 6–7 (emphasis added). Specifically, the Examiner finds, it is “unclear” whether the claimed “pre-processing is external to the IC as a whole or [external to] a particular part of the IC” such as the core, register(s), or other elements recited in the claim or illustrated in the figures. *Id.* Appellants contend the Examiner erred because, according to Appellants, a “person of ordinary skill in the art would clearly appreciate that the external processing is external *to the monolithic IC secure hashing device.*” App. Br. 8 (emphasis added). Appellants contend the portions of the Specification cited above, in the

discussion of the written description rejection, support Appellants' interpretation of "external." We, however, are not persuaded by Appellants' argument.

As discussed above, Appellants' Specification discloses that preprocessing may be done "in software," Spec. ¶¶ 31–33, but does not define preprocessing as being "external" to any element. The claim itself is silent on this point. Before reciting the term "external," claim 12 recites a number of elements including an IC secure hashing device, various registers, a processor, and a wrapper file. App. Br. 19 (Claims App'x). As the Examiner finds, the claim's recitation of "external" could conceivably refer to any of the foregoing, previously recited elements in the claim. Ans. 5. Where, as here, "a claim is amenable to two or more plausible claim constructions, the [Office] is justified in requiring the applicant to more precisely define the metes and bounds of the claimed invention by holding the claim unpatentable under 35 U.S.C. § 112, second paragraph, as indefinite." *Ex parte Miyazaki*, 89 USPQ2d 1207, 1211–12 (BPAI 2008) (precedential); *see also In re Morris*, 127 F.3d 1048, 1056 (Fed. Cir. 1997) (it "is the [A]pplicants' burden to precisely define the invention, not the PTO's").

Accordingly, we sustain the Examiner's rejection of claim 12 under pre-AIA 35 U.S.C. § 112, second paragraph as indefinite.

35 U.S.C. § 103(a) Rejection of Claims 1 and 19

Appellants argue claims 1 and 19 as a group, with claim 1 representative of the group. App. Br. 8–10; *see* 37 C.F.R. § 41.37(c)(iv). Appellants contend the Examiner erred in finding the prior art, specifically

Crispin, teaches a “processor integrated with said plurality of registers [including a mode register configured to store a mode of operation value],” said processor configured to “select a given secure hash algorithm (SHA) variant based upon the mode of operation value,” as recited in claim 1. App. Br. 8–10. We disagree.

As the Examiner finds, Crispin teaches a hashing unit within (i.e., integrated with) a microprocessor, the hashing unit including a “hash control register” containing a *value* indicating the “prescribed hash *mode*” (used to determine how to hash a given message). Ans. 6 (emphasis added) (citing Crispin ¶¶ 53–54). The hash mode field “specifies which SHA mode will be implemented during execution.” *Id.* (citing Crispin ¶ 54). Notwithstanding the slight differences in nomenclature, the Examiner finds, and we agree, the foregoing elements in Crispin correspond to Appellants’ mode register, mode of operation value, and selection of a given SHA as recited in claim 1. *Id.*; *see also* Crispin ¶¶ 51, 55. Thus, on the record before us, we discern no error in the Examiner’s finding that Crispin teaches a processor configured as claimed by Appellants.

Appellants also contend the Examiner erred in finding a rationale to combine the references. App. Br. 12. Appellants argue one of ordinary skill would not combine Sklavos with Crispin “to allow selection of a proper SHA mode” because, Appellants allege, “Sklavos [like Crispin] already provides a method to switch between SHA variants.” *Id.* at 13. As the Examiner finds, however, “[w]hile the end results may be similar[,] the process for obtaining that result is different. . . . Simply because both references are geared toward solving the same problem does not mean they are not combinable.” Ans. 6–7. Indeed, sharing the “same purpose,” “goal,”

or “objective” is sufficient reason for combining the references. *Innovention Toys, LLC v. MGA Entertainment, Inc.*, 637 F.3d 1314, 1322–23 (Fed. Cir. 2011). Moreover, the Examiner finds the use of mode registers, such as in Crispin, would be obvious for one of ordinary skill to try in the system of Sklavos, because mode registers were known to one of ordinary skill and would lead to anticipated success in the selection of SHA mode. Ans. 7; Non-Final Act. 9–10; see *Wm. Wrigley Jr. Co. v. Cadbury Adams USA LLC*, 683 F.3d 1356, 1365 (Fed. Cir. 2012) (“a person of ordinary skill in the art would find it ‘obvious to try’ the combination” of references). On the record before us, we discern no error in the Examiner’s findings.²

Accordingly, we sustain the Examiner’s rejection of claims 1 and 19 under pre-AIA 35 U.S.C. § 103(a) as unpatentable over Sklavos, Horanzy, and Crispin.

35 U.S.C. § 103(a) Rejection of Claim 12

Appellants argue the Examiner erred in rejecting claim 12 because one of ordinary skill in the art would not be motivated to combine the references. App. Br. 14–15. Specifically, Appellants argue the Examiner has provided no rationale for adding the direct memory access (DMA) “interface” of Wheeler to the SHA unit taught by the combination of

² The Examiner also finds, and Appellants do not dispute, the substitution of Crispin’s mode control registers in Sklavos’ system reflects simple “[s]ubstitution of one known element for another to obtain predictable results.” Ans. 7 (citing *In re Fout*, 675 F.2d 297, 301 (CCPA 1982)).

Sklavos and Crispin. *Id.* at 14–15; Non-Final Act. 13–14.³ We are not persuaded.

The Examiner finds a DMA “interface” for receiving data is known in the art, and that one of ordinary skill would understand the benefit of “adding a[] DMA interface” to a SHA unit (such as that in Sklavos) in order to more “efficiently receive[] data” for hashing. Ans. 8; Non-Final Act. 14. On the record before us, we discern no error in the Examiner’s findings. Appellants acknowledge “each applied SHA prior art reference of record receives data for hashing.” App. Br. 15. Simply adding an *interface* (i.e., the interface in Wheeler) to receive data in a SHA unit (i.e., the Sklavos-Crispin combination) is, as the Examiner finds, a predictable variation of hash apparatus design, based on known elements and the design incentive of efficiency. Ans. 8; *Dow Jones & Co., Inc. v. Abblaise, LTD*, 606 F.3d 1338, 1351–52 (Fed. Cir. 2010); *see also KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) (in an obviousness analysis, Board may “take account of the inferences and creative steps that a person of ordinary skill in the art would employ”).

Appellants nevertheless argue that, even if the references are combinable, claim 12 is patentable for the same reasons as claims 1 and 19. App. Br. 14. We, however, are not persuaded for the reasons discussed above.

³ We do not understand Appellants’ argument to rely on the terms “external preprocessing” or “wrapper file,” which were subject to the rejections under 35 U.S.C. § 112 discussed above. Accordingly, the indefinite terms herein do not preclude us from addressing the merits of Appellants’ obviousness argument.

Accordingly, we sustain the Examiner's rejection of claim 12 under pre-AIA 35 U.S.C. § 103(a) as unpatentable over Sklavos, Crispin, and Wheeler.

35 U.S.C. § 103(a) Rejections of Remaining Claims

Appellants do not argue any of the obviousness rejections pertaining to the remaining claims, all of which are dependent. Accordingly, because we sustain the rejection of independent claims 1, 12, and 19, we also sustain the obviousness rejections of the dependent claims.

DECISION

We AFFIRM the Examiner's rejections of claims 1–3, 5, 7–17, and 19–23.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1). *See* 37 C.F.R. § 41.50(f).

AFFIRMED