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.
14/577,148	12/19/2014	Wil Michiels	81641874US01	1008

65913 7590 01/31/2020

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

EXAMINER	
POPHAM, JEFFREY D	

ART UNIT	PAPER NUMBER
2432	

NOTIFICATION DATE	DELIVERY MODE
01/31/2020	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 WIL MICHIELS and JAN HOOGERBRUGGE

Appeal 2019-000001
Application 14/577,148
Technology Center 2400

Before DENISE M. POTHIER, CATHERINE SHIANG, and JOYCE CRAIG, *Administrative Patent Judges*.

SHIANG, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellant[1] appeals under 35 U.S.C. § 134(a) from the Examiner's rejection of claims 1–7 and 29–33, which are all the claims pending and rejected in the application. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm.

[1] We use "Appellant" to refer to "applicant" as defined in 37 C.F.R. § 1.42. Appellant identifies NXP Semiconductors as the real party in interest. Appeal Br. 3.

STATEMENT OF THE CASE

Introduction

The present invention relates to "binding software components that perform a cryptographic function to a reduced secure element." Spec. ¶ 1.

> Various exemplary embodiments relate to a non-transitory machine-readable storage medium encoded with instructions for a keyed cryptographic operation having a first and second portion for execution by a cryptographic system mapping an input message to an output message, including: instructions for outputting first cryptographic data from a first portion the cryptographic operation to a secure hardware device implementing a secure function on the data; instructions for receiving output data from the secure hardware device; instructions for implementing an inverse of the secure function on the output data; and instructions for performing a second portion of the cryptographic operation on the inverted output data, wherein the instructions for implementing an inverse of the secure function on the output data are securely merged with the instructions for performing the second portion of the cryptographic operation on the inverted output data so that the inverted output is not accessible to an attacker.

Spec. ¶ 12. Claims 1 and 29 are exemplary:

> 1. A non-transitory machine-readable storage medium encoded with instructions for a keyed cryptographic operation having first and second portions for execution by a cryptographic system mapping an input message to an output message, comprising:
>
> instructions for outputting first cryptographic data from the first portion of the cryptographic operation to a secure hardware device implementing a secure function on the data;

instructions for receiving output data from the secure hardware device;

instructions for implementing an inverse of the secure function on the output data to produce inverted output data;

instructions for performing a second portion of the cryptographic operation on the inverted output data; and

instructions for outputting second cryptographic data from the first portion of the cryptographic operation directly to the second portion of the cryptographic operation, bypassing the secure hardware device,

wherein the instructions for implementing an inverse of the secure function on the output data are securely merged with the instructions for performing the second portion of the cryptographic operation on the inverted output data so that the inverted output data is not accessible to an attacker.

29. A white-box cryptographic system for performing a keyed cryptographic operation mapping an input message to an output message, the system comprising:

a processor configured to implement a secure hardware device, a secure function implemented in the secure hardware device, wherein,

the system is configured to output first cryptographic data from a first portion of the keyed cryptographic operation to the secure hardware device,

the secure hardware device configured to implement the secure function on the first cryptographic data to produce output data,

the system configured to implement an inverse of the secure function on the output data to produce inverted output data,

the system configured to implement a second portion of the cryptographic operation on the inverted output data, and

the system configured to output second cryptographic data from the first portion of the cryptographic operation directly to the second portion of the cryptographic operation, the second cryptographic data bypassing the secure hardware device,

wherein the implementation of the inverse of the secure function is securely merged with the implementation of the second portion of the cryptographic operation on the inverted output data so that the inverted output data is not accessible to an attacker.

References and Rejections[2]

The Examiner rejects claims 1–7 and 29–33 under 35 U.S.C. § 112(b) as being indefinite for failing to particularly point out and distinctly claim the subject matter that the inventor regards as the invention. Final Act. 20–25.

The Examiner rejects claims 29–33 under 35 U.S.C. § 112(a) for lack of enablement. Final Act. 22–23.

The Examiner rejects claims 1–6 and 29–32 under 35 U.S.C. § 103 as being obvious over the collective teachings of Ciet (US 2009/0252327 A1, published October 8, 2009) and Michiels (US 2012/0093313 A1, published April 19, 2012). Final Act. 26–33.

The Examiner rejects claims 7 and 33 under 35 U.S.C. § 103 as being obvious over the collective teachings of Ciet, Michiels, and ARM (TrustZone® System Security by ARM, The Architecture for the Digital World®, pp. 1–6 (November 21, 2013), http://web.archive.org/web/20131121212920/http://www.arm.com/products/processors/technologies/trustzone/index.php (last viewed January 23, 2020)). Final Act. 33–34.

[2] Throughout this opinion, we refer to the (1) Final Office Action dated March 12, 2018 ("Final Act."); (2) Appeal Brief dated June 4, 2018 ("Appeal Br."); (3) Examiner's Answer dated September 10, 2018 ("Ans."); and (4) Reply Brief dated October 1, 2018 ("Reply Br.").

ANALYSIS

35 U.S.C. § 112(b)

The Examiner determines: "Claims 1–7 and 29–33 are rejected under 35 U.S.C. 112(a) and 112(b) . . . as being indefinite for failing to particularly point out and distinctly claim the subject matter which the inventor or a joint inventor, or for pre-AIA the applicant regards as the invention" with respect to various claim elements (discussed below). Final Act. 20–25.

While the Examiner refers to 35 U.S.C. § 112(a), indefiniteness rejections are governed by 35 U.S.C. § 112(b). Therefore, we assume the reference to 35 U.S.C. § 112(a) is a typographical error.

I

The Examiner rejects claims 1–7 and 29–33 under 35 U.S.C. § 112(b) as being indefinite with respect to the claimed "inverse" of the secure function. *See* Final Act. 20–22. In particular, the Examiner determines:

> Applicant has clearly and explicitly stated that multiplication is not an inverse of division. However, one of ordinary skill in the art would understand that multiplication is the inverse of division. Therefore, Applicant appears to be arguing that the claimed inverse is somehow different from the normal definition of inverse. The claim is indefinite, since the claim cannot be construed using the normal definition of inverse (based on Applicant's allegation that the claimed inverse operation is different from the normal definition of inverse, in particular, alleging that "'multiplication' is not an inverse of the described 'division'", which is the opposite of how one of ordinary skill in the art would understand inverses and inverse operations), but must be construed using the normal

> definition, since the application as originally filed does not provide any specific definition of inverse or inverse function that is different than the ordinary definition. These 2 interpretations of inverse are incompatible since Applicant has explicitly alleged that multiplication is not the inverse of division and it appears as though the interpretation of "inverse" has been irreparably changed based on Applicant's remarks that inverse functions are not inverse functions. Applicant must, in response to this rejection, provide basis for Applicant's abnormal definition of inverse (e.g., that multiplication is not the inverse of division) in the application as originally filed.

Final Act. 21–22 (emphases omitted); *see also* Ans. 5–11.

We disagree with the Examiner. "The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention." 35 U.S.C. § 112(b).

We apply the indefiniteness test approved by *In re Packard*, 751 F.3d 1307 (Fed. Cir. 2014) (per curiam): "[a] claim is indefinite when it contains words or phrases whose meaning is unclear," and "claims are required to be cast in clear–as opposed to ambiguous, vague, indefinite–terms." *See Packard*, 751 F.3d at 1310, 1313; *Ex parte McAward*, Appeal No. 2015-006416 (PTAB Aug. 25, 2017) (precedential) at *8–11 (explaining because of different approaches to indefiniteness before the PTAB and the courts, the PTAB continues to follow *Packard* after the Supreme Court's *Nautilus, Inc. v. Biosig Instruments, Inc.*, 572 U.S. 898 (2014) decision).

> [W]hen the USPTO has initially issued a well-grounded rejection that identifies ways in which language in a claim is ambiguous, vague, incoherent, opaque, or otherwise unclear in describing and defining the claimed invention, and thereafter the applicant fails to provide a satisfactory response, the

> USPTO can properly reject the claim as failing to meet the statutory requirements of § 112(b).

Packard, 751 F.3d at 1311.

We have reviewed the record, and the record fails to show the Appellant has argued multiplication is not the inverse of division. Nor has Appellant argued the claimed "inverse" requires a special definition. Further, Appellant clarifies

> the appellant argued that "Ciet et al. does not show or suggest the claimed "inverse of the secure function" and the claimed "perform a second portion of the cryptographic operation on the inverted output data." The examiner has taken that to mean the appellant has argued a different definition of "inverse". The appellant did not provide any arguments that require a definition different from the normal definition of inverse.

Appeal Br. 7.

In short, the Examiner has not shown the meaning of "inverse" in the claims is unclear to one skilled in the art. *See Packard*, 751 F.3d at 1310.

Because the Examiner has not provided sufficient basis for the rejection, we reverse the Examiner's rejection of claims 1–7 and 29–33 under 35 U.S.C. § 112(b).

II

The Examiner determines:

> Claim 29 states "wherein the implementation of the inverse of the secure function is securely merged with the implementation of the second portion of the cryptographic operation on the inverted output data so that the inverted output data is not accessible to an attacker". However, the claim includes limitations reading "the system configured to

> implement an inverse of the secure function on the output data to produce inverted output data" and "the system configured to implement a second portion of the cryptographic operation on the inverted output data". Therefore, the claimed system is already configured to implement both the inverse and the second portion and, thus, both are already merged into a single system. It is unclear just what effect the final limitation has on the scope of the claim, since it appears to merely be directed to something that already inherently occurs when the same system performs both steps. Claims 30-33 are dependent from claim 29 and are rejected for the same reasons.

Final Act. 23; *see also* Ans. 16–17.

It is well established that during examination, claims are given their broadest reasonable interpretation consistent with the specification and should be read in light of the specification as it would be interpreted by one of ordinary skill in the art, but without importing limitations from the specification. *See In re Am. Acad. of Sci. Tech Ctr.*, 367 F.3d 1359, 1364 (Fed. Cir. 2004) (citations omitted); *SuperGuide Corp. v. DirecTV Enters., Inc.*, 358 F.3d 870, 875 (Fed. Cir. 2004).

Contrary to the Examiner's interpretation, the limitations "the system configured to implement an inverse of the secure function on the output data to produce inverted output data" and "the system configured to implement a second portion of the cryptographic operation on the inverted output data" do not require the instructions to be securely merged. Therefore, the limitation "wherein the instructions for implementing an inverse of the secure function on the output data are securely merged with the instructions for performing the second portion of the cryptographic operation on the inverted output data so that the inverted output data is not accessible to an attacker" further limits the claims by reciting the "securely merged"

language. In short, the Examiner has not shown one skilled in the art would understand that the wherein clause "contains words or phrases whose meaning is unclear." *Packard*, 751 F.3d at 1310.

Because the Examiner has not provided sufficient basis for the rejection, we reverse the Examiner's rejection of claims 29–33 under 35 U.S.C. § 112(b).

III

The Examiner determines:

> Claim 29 is directed to a system comprising a processor configured to implement a secure hardware device. The claim then goes on to describe functionality of the system, such as "the system configured implement an inverse of the secure function on the output data to produce inverted output data" in response to "the secure hardware device configured to implement the secure function on the first cryptographic data to produce output data". However, the only component of the system is, itself, the processor that implements the secure hardware device. . . . . Claims 29-33 are additionally rejected under 35 U.S.C. 112(b), since as the claim stands, the processor must be both trusted and untrusted, is the only component within the system, and must, therefore, perform all functions of the claim, but cannot perform all functions of the claim.

Final Act. 22–23; *see also* Ans. 12–16.

We disagree with the Examiner's interpretation of the claims. Because the claims recite "[a] white-box cryptographic system for performing a keyed cryptographic operation mapping an input message to an output message, the system *comprising* . . ." (emphasis added), the claims are non-limiting and open-ended. *See Gillette Co. v. Energizer Holdings,*

Inc., 405 F.3d 1367, 1371 (Fed. Cir. 2005) ("claim 1 uses the 'open' claim term[] 'comprising' . . . in addition to other language, to encompass subject matter beyond [the explicitly recited limitations]"). Therefore, the system includes—but is not limited to—the claimed processor, and the claimed processor is not "the only component within the system," as the Examiner asserts (Final Act. 23). Nor has the Examiner persuasively explained why the processor "must be both trusted and untrusted . . . [and] perform all functions of the claim, but cannot perform all functions of the claim," as the Examiner asserts (Final Act. 23). In short, the Examiner has not shown the meaning of the claimed "processor" is unclear to one skilled in the art. *See Packard*, 751 F.3d at 1310.

Because the Examiner has not provided sufficient basis for the rejection, we reverse the Examiner's rejection of claims 29–33 under 35 U.S.C. § 112(b).

IV

The Examiner determines:

> Claim 1 is directed to a storage medium having "instructions for" performing various functions. However, Applicant has persistently argued that these instructions must necessarily be executed and their corresponding functions performed. For example, in the response dated 4/10/2017, Applicant has alleged that "According to claim 1, an inverse of the secure function is implemented" (page 12), "A second portion of the cryptographic operation is performed" (page 12), "outputting second cryptographic data . . ." (page 12 and 14). Therefore, Applicant believes that claim 1 requires at least implementing an inverse of the secure function, a second portion of the cryptographic operation, and outputting of the

> second cryptographic data. However, the claim merely states that instructions for such are provided on a medium. It is unclear how this claimed non-transitory machine-readable storage medium may possibly perform such functions. Therefore, while claim 1 states that only instructions are provided, Applicant has alleged that the functions performed by the instructions must actually be performed. Therefore, one cannot ascertain the scope of the claim, since it is unclear whether the medium requires instructions stored thereon or is actually required to perform the inverse function, second portion, and outputting of specific data. Claim 29 has a similar issue and is rejected for the same reasons. All dependent claims are also rejected for the same reasons.

Final Act. 24 (original emphases omitted); *see also* Ans. 17–18.

First, the Examiner misreads claim 29 and the associated dependent claims, because such claims do not recite "a storage medium having 'instructions for' performing various functions," as the Examiner asserts (Final Act. 24).

Second, each of claim 1 and associated dependent claims recites "[a] non-transitory machine-readable storage medium encoded with instructions for a keyed cryptographic operation having first and second portions for execution by a cryptographic system mapping an input message to an output message, comprising . . . ." A "storage medium encoded with instructions" for performing various processes is a well-known claim form, and one skilled in the art would know how to interpret such claims. *See, e.g.*, *Finjan, Inc. v. Secure Computing Corp*., 626 F.3d 1197, 1204–05 (Fed. Cir. 2010) ("the claims at issue are . . . 'storage medium' claims, which do not require the performance of any method steps"; "The storage medium claims . . . cover capability. Claim 65 . . . recites a 'computer-readable storage medium storing program code for causing a server that serves as a gateway to a client

to perform the steps of: receiving . . .; comparing . . .; and preventing execution . . . .' This language does not require that the program code be 'active,' only that it be written 'for causing' a server . . . to perform certain steps"). In short, the Examiner has not shown the meaning of a "storage medium encoded with instructions" for performing various processes is unclear to one skilled in the art. *See Packard*, 751 F.3d at 1310.

Because the Examiner has not provided sufficient basis for the rejection, we reverse the Examiner's rejection of claims 1–7 and 29–32 under 35 U.S.C. § 112(b).

V

The Examiner determines:

> Claim 1 includes "instructions for implementing an inverse of the secure function on the output data to produce inverted output data". However, the inverse of a secure function will rarely result in inverted output data. Therefore, not every implementation of an inverse of a secure function will result in inverted output data. The output data may be "4", arrived at by adding 2 and 2. The inverse of addition being subtraction, the inverse operation would subtract some data from 4, either 2 or otherwise. However, assuming that 2 is subtracted from 4, the result is 2, which is most certainly not the inverse of 4. Therefore, the claim is indefinite, since implementation of the inverse of a secure function will not always result in inverted output data. Claim 29 has a similar issue and is rejected for the same reasons. All dependent claims are also rejected for the same reasons.

Ans. 24–25; *see also* Ans. 19–20.

We disagree with the Examiner, as one skilled in the art would understand the meaning of "instructions for implementing an inverse of the

secure function on the output data to produce inverted output data." Specifically, one skilled in the art would understand the claimed "inverted output data" are produced from "implementing an inverse of the secure function on the output data," and the results of that implementation are the claimed "inverted output data." As a result, the Examiner has not shown the claimed "instructions for implementing an inverse of the secure function on the output data to produce inverted output data" limitation "contains words or phrases whose meaning is unclear" to one skilled in the art. *Packard*, 751 F.3d at 1310.

Because the Examiner has not provided sufficient basis for the rejection, we reverse the Examiner's rejection of claims 1–7 and 29–32 under 35 U.S.C. § 112(b).

VI

The Examiner determines:

> Claim 29 attempts to reference "the output data". However, it is unclear which output data is being referenced, since claim 29 includes at least "output first cryptographic data" and "implement the secure function on the first cryptographic data to produce output data". It is entirely unclear which of these is being referenced later on with respect to "the output data" (and also for anything based thereon, such as "the inverted output data" which, in addition to the issue described above with respect to claim 1, is also indefinite since it is unclear which output data is being referenced). Claims 30-33, dependent from claim 29 are rejected for the same reasons.

Final Act. 25; *see also* Ans. 20–21.

We disagree. Claim 29 recites "the secure hardware device configured to implement the secure function on the first cryptographic data to produce *output data*" and "the system configured to implement an inverse of the secure function on *the output data* to produce inverted output data" (emphases added). Therefore, claim 29 provides the requisite antecedent basis for the claimed "output data" and one skilled in the art would understand how to interpret that claim limitation.

Further, claim 29 recites "the system configured to implement an inverse of the secure function on the output data to produce *inverted output data*" and "the system configured to implement a second portion of the cryptographic operation on *the inverted output data*" (emphases added). Therefore, the claim provides the requisite antecedent basis for the claimed "inverted output data" and one skilled in the art would understand how to interpret that claim limitation. As a result, the Examiner has not shown the meanings of the "output data" and the "inverted output data" are unclear to one skilled in the art. *See Packard*, 751 F.3d at 1310.

Because the Examiner has not shown sufficient basis for the rejection, we reverse the Examiner's rejection of claims 29–33 under 35 U.S.C. § 112(b).

35 U.S.C. § 112(a)

The Examiner determines:

> Claim 29 is directed to a system comprising a processor configured to implement a secure hardware device. The claim then goes on to describe functionality of the system, such as "the system configured implement an inverse of the secure function on the output data to produce inverted output data" in

> response to "the secure hardware device configured to implement the secure function on the first cryptographic data to produce output data". However, the only component of the system is, itself, the processor that implements the secure hardware device. Thus, this appears to mean that the processor sends and receives data to and from itself (e.g., between the portions of the claim that are performed by the secure hardware device, which is implemented on/in the processor and the rest of the claim, which is performed by the system which solely includes this processor implementing the secure hardware device), which does not make sense in the realm of secure computing, where one portion of the system is intended to be trusted and the other is not, since *the same processor would be both trusted and untrusted*, which does not appear to be possible (there is certainly no description of such a trusted and un-trusted processor in the application). It appears as though the claim is missing an essential component, i.e., the component(s) that sends and receives data to/from the secure hardware device. Thus, claims 29-33 are rejected under 35 U.S.C. 112(a) or 35 U.S.C. 112 (pre-AIA), first paragraph, as based on a disclosure which is not enabling. See *In re Mayhew*, 527 F.2d 1229, 188 USPQ 356 (CCPA 1976).

Final Act. 22–23.

We disagree. "The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same." 35 U.S.C. § 112(b).

The test of enablement is whether without undue experimentation, one skilled in the art could make or use the invention from the disclosures coupled with information known in the art. *See In re Antor Media Corp.*, 689 F.3d 1282, 1289 (Fed. Cir. 2012); *U.S. v. Telectronics, Inc.*, 857 F.2d

778, 785 (Fed. Cir. 1988) (citation omitted). In *Mayhew*, the Federal Circuit determines:

> Although appellant now strenuously argues that the cooling bath is optional, his specification not only fails to support this contention, but leads us, as it did the examiner and board, to believe that both it and its location are essential. We therefore conclude that claims which fail to recite the use of a cooling zone, specially located, are not supported by an enabling disclosure.

In re Mayhew, 527 F.2d 1229, 1233.

Because the claims recite "[a] white-box cryptographic system for performing a keyed cryptographic operation mapping an input message to an output message, the system *comprising* . . ." (emphasis added), the system includes—but is not limited to—the claimed processor. Therefore, the claimed processor is not "the only component within the system," and is not required to be "both trusted and untrusted" (Final Act. 23). Unlike the situation in *Mayhew*, the Examiner has not provided sufficient evidence from the Specification to show the claims lack essential elements. As a result, the Examiner has not shown "the claim is missing an essential component" (Final Act. 22), and, therefore, has not provided sufficient basis for the enablement rejection. *See Mayhew*, 527 F.2d at 1233.

Accordingly, we reverse the Examiner's rejection of claims 29–33 under 35 U.S.C. § 112(a).

Obviousness

On this record, the Examiner did not err in rejecting claim 1.

We disagree with Appellant's arguments. To the extent consistent with our analysis below, we adopt the Examiner's findings and conclusions in (i) the action from which this appeal is taken and (ii) the Answer.[3]

I

Appellant contends:

> Ciet et al. does not show or suggest the claim 1 limitations "instructions for receiving output data from the secure hardware device" and "instructions for implementing an inverse of the secure function on the output data to produce inverted output data." The inverse of Ciet et al. is of the "secret value", see for example, Ciet et al. at paragraph 0025. Ciet et al. teaches at paragraph 0021 that the secret is a random value. Whereas, the present invention, as claimed in claim 1, includes instructions for implementing an inverse of the secure function on output data to produce inverted output data. Also, the output data is claimed to be received from the secure hardware device. Ciet et al. does not disclose where the secret originates, but says at paragraph 0021 that it is a "secure scalar value", not a secure function as in, for example, claim 1.

Appeal Br. 10.

Appellant has not persuaded us of error, because Appellant's arguments are not directed to the Examiner's specific findings. As pointed out by the Examiner,

> Appellant is making allegations regarding an inverted secret value, which is not an inverse function. The rejection made clear that the instructions for implementing an inverse of the

[3] To the extent Appellant advances new arguments in the Reply Brief without showing good cause, Appellant has waived such arguments. *See* 37 C.F.R. § 41.41(b)(2).

> secure function on the output data is met by "performing the inverse of any operation performed in function **P** within function **N** in the white box, such as RSA signature verification" [in Ciet.] The rejection did not state that the inverse of the secure function was an inverted secret value.

Ans. 22.

> Instructions for implementing an inverse of the secure function on the output data to produce inverted output data (Abstract; Paragraphs 15- 25 and 29-37; performing the inverse of any operation performed in function P within function N in the white box, such as RSA signature verification, in step 4 of the reference cited in paragraph 31 of Ciet, etc., as examples).

Final Act. 27.

II

Appellant contends:

> Ciet et al. does not show or suggest the claim limitation "wherein the instructions for implementing an inverse of the secure function on the output data are securely merged with the instructions for performing the second portion of the cryptographic operation on the inverted output data so that the inverted output data is not accessible to an attacker". As discussed above, Ciet et al. does not disclose "inverse of the secure function". Ciet et al. only shows the inverse of a scalar value (paragraphs 0021 and 0025). Also, Ciet el al. does not say that the instructions for implementing an inverse of the secure function are securely merged with the instructions for performing the second portion. Ciet el al. only discloses implementations of the functions P, M, and N, but does not disclose a relationship between the functions such as the claimed instructions for implementing an inverse of the secure function on the output data being securely merged with the instructions for performing the second portion of the

> cryptographic operation on the inverted output data so that the inverted output data is not accessible to an attacker.

Appeal Br. 10–11; *see also* Reply Br. 8.

In response to Appellant's arguments, the Examiner further explains:

> The rejection of claim 1 made clear that the final limitation was met by Ciet's disclosure of "function N performs both the inverse of a function within function P as well as the additional functions described therein, such as in computing the exponentiation using the now available m' as well as the signature verification, for example".
>
> It is noted that the claimed "instructions for performing a second portion of the cryptographic operation" that is merged with the instructions for implementing an inverse of the secure function is quite broad. Any operation whatsoever could meet this "second portion" since the claim does not define what is within this second portion. Any single addition, multiplication, XOR, NOR, OR, AND, move, subtraction, division, reception, or any other operation could be within this claimed second portion.
>
> As the rejection made clear one example of what is performed in function N() that shows that function N() includes both an inverse of a secure function and a second portion of the cryptographic operation (e.g., signature verification and computing an exponentiation using m') and Appellant has provided no argument there against, it is clear that Ciet discloses the merging of the instructions.
>
> Additionally, Ciet makes clear that both M() (paragraph 18) and N() (paragraph 20) could be executed in a white box, while P() could be executed in a black box (paragraph 19). Thus, M() and N() are securely merged within the white box as well. This shows that the first portion (e.g., at least one operation performed in M( )) is associated with the second portion (e.g., at least one operation performed in N( )).

Ans. 25–26.

Appellant fails to persuasively respond to such explanation and, therefore, fails to show Examiner error. *See In re Baxter Travenol Labs.*, 952 F.2d 388, 391 (Fed. Cir. 1991) ("It is not the function of this court [or this Board] to examine the claims in greater detail than argued by an appellant, looking for [patentable] distinctions over the prior art.").

Further, Appellant's attorney arguments about Ciet and Michiels (Appeal Br. 11; Reply Br. 8) are unpersuasive, as Appellant does not provide sufficient objective evidence to support such arguments. *See In re Geisler*, 116 F.3d 1465, 1470 (Fed. Cir. 1997) ("attorney argument [is] not the kind of factual evidence that is required to rebut a prima facie case of obviousness"); *Meitzner v. Mindick*, 549 F.2d 775, 782 (CCPA 1977) ("Argument of counsel cannot take the place of evidence lacking in the record.").

III

Appellant argues:

> Michiels does not disclose either a secure entity or a secure hardware device as claimed. Michiels generally discloses the use of lookup tables in the computation of a cryptography algorithm in a white box implementation. The white box implementation of Michiels does not disclose the use of a secure entity or a secure hardware device as claimed.

Appeal Br. 11.

Appellant has not persuaded us of error, because Appellant's arguments are not directed to the Examiner's specific findings. As pointed out by the Examiner (Ans. 26), because the Examiner cites Ciet for teaching

the claimed "secure hardware device," Michiels does not need to teach that element.

Further, Appellant's arguments about "a secure entity" (App. Br. 11) are not commensurate with the scope of the claims, as the claims do not recite that term.

Because Appellant has not persuaded us the Examiner erred, we sustain the Examiner's obviousness rejection of independent claim 1.

Appellant argues "independent claim 29 . . . [is] patentable for at least the same reasons." Appeal Br. 12. The Examiner applies the same findings and conclusions (discussed above) to claim 29. *See* Final Act. 30. Therefore, for similar reasons, we sustain the Examiner's obviousness rejection of independent claim 29.

We also sustain the Examiner's obviousness rejection of dependent claims 2–7 and 30–33, as Appellant does not advance separate substantive arguments about those claims.

CONCLUSION

We reverse the Examiner's decision rejecting claims 1–7 and 29–33 under 35 U.S.C. § 112(b).

We reverse the Examiner's decision rejecting claims 29–33 under 35 U.S.C. § 112(a).

We affirm the Examiner's decision rejecting claims 1–7 and 29–33 under 35 U.S.C. § 103.

Because we affirm at least one ground of rejection with respect to each claim on appeal, we affirm the Examiner's decision rejecting claims 1–7 and 29–33. *See* 37 C.F.R. § 41.50(a)(1).

DECISION SUMMARY

Claims Rejected	**35 U.S.C. §**	**Reference(s)/Basis**	**Affirmed**	**Reversed**
1–7, 29–33	112(b)	Indefiniteness		1–7, 29–33
29–33	112(a)	Enablement		29–33
1–6, 29–32	103	Ciet, Michiels	1–6, 29–32	
7, 33	103	Ciet, Michiels, ARM	7, 33	
Overall Outcome			1–7, 29–33	

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)(iv). *See* 37 C.F.R. § 41.50(f).

AFFIRMED