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.
12/514,922	05/14/2009	Wilhelmus Petrus Adrianus Johannus Michiels	14-30139-US	4928

98804 7590 12/27/2016

Reed Smith LLP
P.O. Box 488
Pittsburgh, PA 15230

EXAMINER	
ALMEIDA, DEVIN E	

ART UNIT	PAPER NUMBER
2492	

NOTIFICATION DATE	DELIVERY MODE
12/27/2016	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):

ptoipinbox@reedsmith.com
mskaufman@reedsmith.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte WILHELMUS PETRUS ADRIANUS JOHANNUS MICHIELS
and
PAULUS MATHIAS HUBERTUS MECHTILDIS ANTONIUS GORISSEN

Appeal 2016-001069
Application 12/514,922[1]
Technology Center 2400

Before ST. JOHN COURTENAY, III, JOHNNY A. KUMAR, and NORMAN H. BEAMER, *Administrative Patent Judges*.

BEAMER, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellants appeal under 35 U.S.C. § 134(a) from the Examiner's Final Rejection of claims 1–5, 7, 8, 10–14, and 16–23. Claims 6, 9, and 15 are cancelled. We have jurisdiction over the pending rejected claims under 35 U.S.C. § 6(b).

We affirm.

---

[1] Appellants identify Irdeto B.V. as the real party in interest. (App. Br. 1.)

THE INVENTION

Appellants' disclosed and claimed invention is directed to a white-box implementation of a cryptographic method. (Spec. 1.) As stated in the Specification:

> White-box cryptography involves implementing a block cipher in software, such that an attacker cannot even extract the key in the white-box attack model. The white-box attack model is among the strongest conceivable attack models, because the attacker is assumed to have full access to the implementation and full control over the execution environment.

(Spec. 13.) Claim 1, reproduced below, is illustrative of the subject matter on appeal:

> 1. A cryptographic method for being implemented in a white-box implementation thereof, the method comprising:
>
> receiving, at an input of a data processing system, a key, the key comprising information representing a diffusion operator;
>
> using one or more processors of the data processing system to apply a plurality of transformations based on the key, each transformation replacing a respective input word by a respective output word; and
>
> using the one or more processors of the data processing system to apply the diffusion operator represented by the information in the key to a concatenation of a plurality of the output words to thereby spread information represented by the output words among the output words.

REJECTIONS

In the Answer, the Examiner entered a new ground of rejection of claims 1–5, 7, 8, 10–14, and 16–23 under 35 U.S.C. § 101 as being directed to non-statutory subject matter. (Ans. 2–3.)

The Examiner rejected claims 1–3, 5, 7, 8, 10–12, 14, and 16–23 under 35 U.S.C. § 102(b) as being anticipated by S. Chow et al., *White-Box Cryptography And An AES Implementation*, 9th Annual Workshop on Selected Areas in Cryptography (SAC '02) (Aug. 2002). (Final Act. 3–5.)[2]

ISSUE ON APPEAL

Appellants' arguments in the Briefs present the following issues:[3]

First Issue: Whether the Examiner erred in finding Chow discloses the limitations of independent claim 1, "the key comprising information representing a diffusion operator [and] apply the diffusion operator represented by the information in the key to a concatenation of a plurality of the output words to thereby spread information represented by the output words among the output words," and the similar limitations recited in independent claims 7 and 10. (App. Br. 3–10.)

Second Issue: Whether the claims are invalid under 35 U.S.C. § 101 as being directed to non-statutory subject matter. (Reply Br. 1–5.)

---

[2] Prior to entering the Section 101 rejection in the Answer, the Examiner objected to claims 4 and 13 as being dependent upon a rejected base claim, and indicated those claims would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. (Final Act. 5.)

[3] Rather than reiterate the arguments of Appellants and the findings of the Examiner, we refer to the corrected Appeal Brief (filed Apr. 17, 2015); the Reply Brief (filed Nov. 2, 2015); the Final Office Action (mailed Aug. 14, 2014); and the Examiner's Answer (mailed Sept. 4, 2015) for the respective details.

ANALYSIS

First Issue

In finding Chow discloses the limitations at issue, the Examiner cites, without specifics, to sections of Chow disclosing a modification of the AES (Advanced Encryption Standard). (Final Act. 3; Chow Fig. 1, Type II, §§ 3.1, 3.3, 3.5.) Although not specifically mentioned in the rejection, those cited portions of Chow include a provision for integrating the AES keys into the AES "*SubBytes*" transformation to create a "T-box," preceded by application of a random "mixing bijection" matrix which introduces diffusion. (Chow Fig. 1, Type II, §§ 3.1, 3.4.)

Appellants argue the Examiner's rejection is insufficient because "the Examiner has cited various sections of the Chow reference but has not provided any explanation regarding which features in Chow are believed to disclose the recited limitations." (App. Br. 4.) Appellants go on to distinguish the aforementioned features of the Chow reference included in the sections cited by the Examiner, but not specifically relied on in the Final Action — namely, the provision in Chow for integrating the AES keys into the AES "SubBytes" transformation, and the application of a random "mixing bijection" matrix which introduces diffusion. (App. Br. 6–9; Chow Fig. 1, Type II, §§ 3.1, 3.3, 3.5.) Appellants argue the integration of the keys into the SubBytes transformation to obtain T-boxes "*are not diffusion operators* as they handle each byte of input separately from the other bytes of the input," and the bijection matrix used to achieve diffusion is "randomly determined" and not represented by information in a key, as required by the claims. (App. Br. 6–7.)

> The Examiner responds:
>
> [T]here is no language recited in Claim 1 that precludes Chow's T-boxes information (i.e. S-boxes, etc.) from being considered as teaching a diffusion operator. . . . Given the broadest reasonable interpretation . . . Claim 1's recitation of "a key comprising information representing a diffusion operator" is taught in Chow section 3.1, where the key is the T-Box that includes the S-Box and the bijection. This key also includes information representing the diffusion operator since when used with MixColumns step it provides diffusion, per its plain and ordinary meaning.

(Ans. 4.) In reply, Appellants argue Claim 1 does preclude T-boxes from being considered a diffusion operator, given the claim requirement to apply the diffusion operator "*to a concatenation of a plurality of the output words to thereby spread information represented by the output words among the output words*," whereas the T-boxes of Chow "are arranged to receive a single word and output a single word." (Reply Br. 7–8.) Appellants also argue neither the MixColumns step nor the bijection matrix, which the Examiner apparently equates to diffusion operators, are not represented by information in a key, as required by the claims. (Reply Br. 9.)

We agree with Appellants that the Examiner's anticipation rejection does not sufficiently map the disclosure of Chow to the claim elements at issue, and the Answer does not sufficiently address the Appellants' arguments. The Examiner does not articulate the broadest reasonable interpretations of "the key comprising information representing a diffusion operator," or "to apply the diffusion operator . . . to a concatenation of a plurality of the output words to thereby spread information represented by the output words among the output words," or the basis for such interpretations. Nor does the Examiner sufficiently explain how the T-

boxes, bijection matrix, MixColumns step, or other features of Chow disclose the subject matter of these claim elements as broadly interpreted.

Therefore, we find to affirm the Examiner's anticipation rejection on this record would require us to engage in speculation as to the nature of, or basis for, the Examiner's construction of the claim elements at issue, or how Chow may disclose the subject matter of the claims as interpreted. We decline to engage in speculation. Therefore, for essentially the same reasons argued by Appellants (App. Br. 4), we are constrained on the record before us to find the Examiner erred in rejecting independent claims 1, 7, and 10 as anticipated by Chow.

Second Issue

The Examiner rejected the claims as directed to non-statutory subject matter, applying the *2014 Interim Guidance on Patent Subject Matter Eligibility* (Federal Register Vol. 79, No. 241, December 2014). (Ans. 2–3.) The Examiner concludes the claims are "directed to the abstract idea of data transformation through mathematical manipulation. . . . [And] recite a diffusion operation that merely employs mathematical relationships to manipulate existing information (i.e. key information and input word) to generate new information (i.e. output words)." (Ans. 2.) Noting the claims include "processors," "memory," and non-transitory "computer-readable storage medium" as implementing the mathematical manipulations, the Examiner concludes these additional elements are "well-understood, routine and conventional activities previously known to the industry" and are not "sufficient to amount to significantly more than the judicial exception because there are no additional elements besides the abstract idea." (Ans. 3.)

Appellants argue the Examiner errs, because the claims are not directed to the "abstract idea of *data transformation through mathematical manipulation*," and that "the Examiner has not specified anywhere in the Examiner's Answer what he believes to be the abstract 'mathematical relationship' which is being employed by the diffusion operation." (Reply Br. 3.) Appellants further argue the claimed subject matter does not "preempt the field of data encryption," given that such established encryption techniques as the prior art AES would not fall under the scope of the claims. (Reply Br. 4.) In addition, Appellants argue, even if the claims are drawn to an abstract idea, they "recite limitations that are 'significantly more' than the abstract idea itself," given the claimed key-based transformations and diffusion operations "results in improved security of the resulting output words and the cryptographic process since the diffusion operation is not independent of the key," which are limitations "*other than what is well-understood, routine and conventional in the field*." (Reply Br. 5–6.)

The Supreme Court has "set forth a framework for distinguishing patents that claim laws of nature, natural phenomena, and abstract ideas from those that claim patent-eligible applications of those concepts." *Alice Corp. Pty. Ltd. v. CLS Banklnt'l*, 134 S.Ct. 2347, 2355 (2014) (citing *Mayo Collaborative Servs. v. Prometheus Labs, Inc.*, 132 S.Ct. 1289, 1296–1297 (2012)). According to the framework, the inquiry must first determine whether the claims at issue are directed to one of those concepts (i.e., laws of nature, natural phenomena, and abstract ideas). *Id.* If so, the second step of the framework is to "consider the elements of each claim both individually and 'as an ordered combination' to determine whether the additional

elements 'transform the nature of the claim' into a patent-eligible application." *Id.* The second step of the framework also is characterized as "a search for an 'inventive concept" — an element or combination of elements sufficient to ensure that the claim amounts to "significantly more" than the abstract idea itself. *Id.*

We agree with the Examiner that the claimed subject matter is directed to a patent ineligible concept, which the Examiner characterizes as "data transformation through mathematical manipulation." (Ans. 2.) We are not persuaded by Appellants' argument that the claims do not fall under this description — the claims are directed to data manipulation algorithms, such as transformation of digital words based on keys, and spreading information amount output words by applying diffusion operators. These algorithms represent abstract mathematical operations that can be performed either mentally or with "pencil and paper." *CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366, 1371 (Fed. Cir. 2011). The algorithmic operations are comparable to computing alarm limits in a catalytic conversion process using a mathematical formula, which was held a patent ineligible abstract idea in *Parker v. Flook*, 437 U.S. 584 (1978). *See Alice*, 134 S.Ct. at 2355.

Appellants' argument that the claims do not preempt the field of encryption are not persuasive. "While preemption may signal patent ineligible subject matter, the absence of complete preemption does not demonstrate patent eligibility." *Ariosa Diagnostics, Inc. v. Sequenom, Inc.*, 788 F.3d 1371, 1379 (Fed. Cir. 2015).

Turning to the second step of the framework, we agree with the Examiner that the recitation of the use of processors and memory in the

claims fails to transform the abstract idea into a patent-eligible invention. As the Supreme Court explains regarding the second step of the framework, "the mere recitation of a generic computer cannot transform a patent-ineligible abstract idea into a patent-eligible invention." *Alice*, 134 S.Ct. at 2358. Stated in other words, "if a [] recitation of a computer amounts to a mere instruction to 'implement [t]' an abstract idea 'on ... a computer,' that addition cannot impart patent eligibility." *Id.* (citing *Mayo*, 132 S.Ct at 1301).

Moreover, we are not persuaded the alleged improved security resulting from the claimed diffusion operation dependence on the key (i.e., "the diffusion operator represented by the information in the key") creates a patent-eligible invention. Although, as discussed above, we do not sustain the Examiner's anticipation rejection, the potentially novel idea of a key-dependent diffusion operator is nonetheless an abstract idea, and the record does not demonstrate the implementation of this idea, as compared to the prior art implementations of the AES encryption standard and the cited Chow articles described in the Specification, is other than "routine and conventional." (Spec. 2–4.)

CONCLUSION

For the reasons stated above, we sustain the Section 101 rejection of the pending claims.

Also for the reasons stated above, we do not sustain the anticipation rejection of independent claims 1, 7, and 10. We also do not sustain the anticipation rejections of claims 2, 3, 5, 8, 11, 12, 14, and 16–23, which claims depend from claims 1, 7, or 10.

DECISION

We affirm the Examiner's Section 101 rejection of claims 1–5, 7, 8, 10–14, and 16–23.

We reverse the Examiner's anticipation rejections of claims 1–3, 5, 7, 8, 10–12, 14, and 16–23.

Because we have affirmed at least one ground of rejection with respect to each claim on appeal, the Examiner's decision is affirmed. *See* 37 C.F.R. § 41.50(a)(1).

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).

AFFIRMED