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.
14/588,505	01/02/2015	Craig B. Gentry	YOR920100500US4	6390

48237 7590 03/29/2018

HARRINGTON & SMITH
4 RESEARCH DRIVE, Suite 202
SHELTON, CT 06484-6212

EXAMINER	
JEUDY, JOSNEL	

ART UNIT	PAPER NUMBER
2438	

NOTIFICATION DATE	DELIVERY MODE
03/29/2018	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):

USPTO@HSPATENT.COM

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte CRAIG B. GENTRY and SHAI HALEVI

Appeal 2017-007680
Application 14/588,505[1]
Technology Center 2400

Before LARRY J. HUME, CATHERINE SHIANG, and
JASON M. REPKO, *Administrative Patent Judges*.

HUME, *Administrative Patent Judge*.

DECISION ON APPEAL

This is a decision on appeal under 35 U.S.C. § 134(a) of the Final Rejection of claims 1–20, which are all claims pending in the application. We have jurisdiction under 35 U.S.C. § 6(b).

We REVERSE.

---

[1] According to Appellants, the real party in interest is International Business Machines Corp. App. Br. 2.

STATEMENT OF THE CASE[2]

The Invention

Appellants' disclosed embodiments and claimed invention "relate generally to encryption and decryption and, more specifically, relate to various encryption and decryption techniques that may be particularly applicable for homomorphic encryption." Spec. 1, ll. 13–15.

Exemplary Claim

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

> 1. A method, comprising:
>
> determining, by a computer system, a public key and a private key by performing at least the following:
>
> computing, by the computer system, a resultant and a free term of a scaled inverse of a first polynomial $v(x)$ modulo a second polynomial $f_n(x)$, where the second polynomial is of a form $f_n(x) = x^n \pm 1$, where $n = 2^k$ and k is an integer greater than 0, at least by performing:
>
> computing lowest two coefficients of a third polynomial $g(z)$ that is a function of the first polynomial and the second polynomial, where $g(z) \triangleq \prod_{i=0}^{n-1}(v(\rho_i) - z)$, where ρ_0, ρ_1, ... , ρ_{n-1} are roots of the second polynomial $f_n(x)$ over a field;
>
> outputting the lowest coefficient of $g(z)$ as the resultant; and

---

[2] Our decision relies upon Appellants' Appeal Brief ("App. Br.," filed Dec. 8, 2016); Reply Brief ("Reply Br.," filed Apr. 10, 2017); Examiner's Answer ("Ans.," mailed Feb. 24, 2017); Final Office Action ("Final Act.," mailed June 9, 2016); and the original Specification ("Spec.," filed Jan. 2, 2015).

> outputting the second lowest coefficient of $g(z)$ divided by n as the free term of the scaled inverse of the first polynomial $v(x)$ modulo the second polynomial $f_n(x)$;
>
> determining, by the computer system, the public key by using at least the resultant;
>
> determining, by the computer system, the private key using the free term of the scaled inverse of the first polynomial $v(x)$ modulo the second polynomial $f_n(x)$;
>
> encrypting, by the computer system, multiple data using the public key;
>
> sending, by the computer system, the encrypted multiple data and public key to a remote computer; and
>
> receiving by the computer system ciphertext from the remote computer and decrypting, by the computer system, the received ciphertext using the private key to create plaintext to be used by the computer system, where the ciphertext is a result of homomorphic operations performed by the remote computer using the encrypted multiple data and the public key.

Rejection on Appeal

Claims 1–20 stand rejected under 35 U.S.C. § 101 as being directed to patent-ineligible subject matter. Final Act. 2–4; *see also* Ans. 7.

CLAIM GROUPING

Based on Appellants' arguments (App. Br. 5 *et seq.*), we decide the appeal of the patent-ineligible subject matter rejection of claims 1–20 on the basis of representative claim 1.

ISSUE

Appellants argue (App. Br. 4–29; Reply Br. 2–10) the Examiner's rejection of claim 1 under 35 U.S.C. § 101 as being directed to patent-ineligible subject matter is in error. These contentions present us with the following issue:

Did the Examiner err in concluding claim 1 is patent-ineligible because it is directed to an abstract idea without significantly more?

ANALYSIS

Based upon our review of the record, we find a preponderance of the evidence supports particular arguments advanced by Appellants with respect to the appealed claims for the specific reasons discussed below. We highlight and address specific findings and arguments regarding claim 1 for emphasis as follows.

We first note, "[w]hether a patent claim is drawn to patent-eligible subject matter is an issue of law that [is] reviewed de novo." *SiRF Tech., Inc. v. Int'l Trade Comm'n*, 601 F.3d 1319, 1331 (Fed. Cir. 2010).

Alice Framework

Section 101 provides that anyone who "invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof" may obtain a patent. 35 U.S.C. § 101. The Supreme Court has repeatedly emphasized that patent protection should not extend to claims that monopolize "the basic tools of scientific and technological work." *Gottschalk v. Benson*, 409 U.S. 63, 67 (1972); *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 71 (2012);

Alice Corp. Pty. v. CLS Bank Int'l, 134 S. Ct. 2347, 2354 (2014). Accordingly, laws of nature, natural phenomena, and abstract ideas are not patent-eligible subject matter. *Id.*

The Supreme Court's two-part *Mayo/Alice* framework guides us in distinguishing between patent claims that impermissibly claim the "building blocks of human ingenuity" and those that "integrate the building blocks into something more." *Alice*, 134 S. Ct. at 2354. First, we "determine whether the claims at issue are directed to a patent-ineligible concept." *Id.* at 2355. If so, we "examine the elements of the claim to determine whether it contains an 'inventive concept' sufficient to 'transform' the claimed abstract idea into a patent-eligible application." *Id.* at 2357 (quoting *Mayo*, 566 U.S. at 72, 79). While the two steps[3] of the *Alice* framework are related, the "Supreme Court's formulation makes clear that the first-stage filter is a meaningful one, sometimes ending the § 101 inquiry." *Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350, 1353 (Fed. Cir. 2016).

Alice Step 1 — Abstract Idea

We note the Supreme Court "has not established a definitive rule to determine what constitutes an 'abstract idea'" for the purposes of step one. *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1334 (Fed. Cir. 2016) (citing *Alice*, 134 S. Ct. at 2357). Our reviewing court has held claims ineligible as being directed to an abstract idea when they merely collect electronic information, display information, or embody mental processes that could be

[3] Applying this two-step process to claims challenged under the abstract idea exception, the courts typically refer to step one as the "abstract idea" step and step two as the "inventive concept" step. *Affinity Labs of Tex., LLC v. DIRECTV, LLC*, 838 F.3d 1253, 1257 (Fed. Cir. 2016).

performed by humans. *Elec. Power Grp.*, 830 F.3d at 1353–54 (collecting cases). At the same time, "all inventions at some level embody, use, reflect, rest upon, or apply laws of nature, natural phenomena, or abstract ideas." *Mayo*, 566 U.S. at 71. Under this guidance, we must therefore ensure at step one that we articulate what the claims are directed to with enough specificity to ensure the step one inquiry is meaningful. *Alice*, 134 S. Ct. at 2354 ("[W]e tread carefully in construing this exclusionary principle lest it swallow all of patent law.").

Appellants contend, "[t]he instant claims are directed in part to an encryption scheme that allows homomorphic operations to take place on data, and are performed on what is commonly referred to as the 'client' system. . . . It is not possible to underestimate the importance of homomorphic encryption techniques." App. Br. 6. "The invention herein is a further improvement on the original techniques for homomorphic encryption." App. Br. 9.

Appellants further allege "[t]he Examiner appears to be dissecting the claim into an 'abstract idea' and possibly conventional parts of the claim, which is not currently the law as described below." App. Br. 10. Further, "while the independent claims involve an algorithm, it is helpful to review the claims without the algorithm. See claim 1, which is chosen to be representative (where '[...]' indicates parts of the algorithm, which have been removed)." *Id.*

Contrary to Appellants' contentions, the Examiner concludes the abstract ideas in claim 1 may be characterized by abstract processing steps the Examiner "interpret[s] as collecting information and using mathematical

procedure for converting one form of numerical representation to another." Final Act. 3.

Under the "abstract idea" step we must evaluate "the 'focus of the claimed advance over the prior art' to determine if the claim's 'character as a whole' is directed to excluded subject matter." *Affinity Labs*, 838 F.3d at 1257 (citation omitted).

Turning to the claimed invention, Appellants' "redacted" claim 1[4] is as follows:

> A method, comprising:
>
> determining, by a computer system, a public key and a private key by performing at least the following:
>
> [...]
>
> determining, by the computer system, the public key [...];
>
> determining, by the computer system, the private key [...];
>
> encrypting, by the computer system, multiple data using the public key;
>
> sending, by the computer system, the encrypted multiple data and public key to a remote computer; and
>
> receiving by the computer system ciphertext from the remote computer and decrypting, by the computer system, the received ciphertext using the private key to create plaintext to be used by the computer system, where the ciphertext is a result of homomorphic operations performed by the remote computer using the encrypted multiple data and the public key.

App. Br. 10.

[4] For purposes of illustration, Appellants present claim 1 in a redacted form without the recited mathematical functions/algorithms. App. Br. 10.

In the Answer, the Examiner responded the steps of claim 1 "are interpreted as a mathematical formula[e]" (Ans. 4), and the additional limitations of encrypting, sending data, and receiving data "are interpreted as an idea 'of itself.'" Ans. 4.

Under step one, we agree with the Examiner that the inventions claimed in each of independent claims 1, 8, and 14 are directed to an abstract idea, i.e., "collecting information and using mathematical procedure for converting one form of numerical representation to another." Final Act. 3.

As the Specification itself observes, "[t]he exemplary embodiments of this invention relate generally to encryption and decryption and, more specifically, relate to various encryption and decryption techniques that may be particularly applicable for homomorphic encryption." Spec. 1, ll. 13–15.[5] We find this type of activity, i.e., mathematical manipulation, no matter how tedious and time-consuming, includes longstanding conduct that existed well before the advent of computers and the Internet, and could be carried out by a human with pen and paper. *See CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366, 1375 (Fed. Cir. 2011) ("That purely mental processes can be unpatentable, even when performed by a computer, was precisely the holding of the Supreme Court in *Gottschalk v. Benson*.").[6]

---

[5] *See also* Spec. 98 ("Abstract") ("In one exemplary embodiment of the invention, a method for computing a resultant and a free term of a scaled inverse of a first polynomial $v(x)$ modulo the second polynomial $f_n(x)$, including . . . "). *See* claim 1 for the specific mathematical steps.

[6] *CyberSource* further guides that "a method that can be performed by human thought alone is merely an abstract idea and is not patent-eligible under § 101." *CyberSource*, 654 F.3d at 1373.

Our reviewing court has previously held other patent claims ineligible for reciting similar abstract concepts. For example, while the Supreme Court has enhanced the § 101 analysis since *CyberSource* in cases like *Mayo* and *Alice*, they continue to "treat[ ] analyzing information by steps people go through in their minds, or by mathematical algorithms, without more, as essentially mental processes within the abstract-idea category." *Synopsys, Inc. v. Mentor Graphics Corp.*, 839 F.3d 1138, 1146–47 (Fed. Cir. 2016) (alteration in original) (quoting *Elec. Power Grp.*, 830 F.3d at 1354).

In this regard, the claims are similar to claims our reviewing court has found patent ineligible in *Electric Power Group*, 830 F.3d at 1353–54 (collecting information and "analyzing information by steps people go through in their minds, or by mathematical algorithms, without more, [are] essentially mental processes within the abstract-idea category").

Therefore, in agreement with the Examiner, we conclude claim 1 involves nothing more than identifying, computing, storing, comparing, and securely outputting data, without any particular inventive technology — an abstract idea. *See Elec. Power Grp.*, 830 F.3d at 1354. We further refer to *Content Extraction*, where the Federal Circuit has provided additional guidance on the issue of statutory subject matter by holding claims to collecting data, recognizing certain data within the collected data set, and storing that recognized data in memory were directed to an abstract idea and therefore unpatentable under § 101. *Content Extraction & Transmission LLC v. Wells Fargo Bank, N.A.*, 776 F.3d 1343 (Fed. Cir. 2014).

Accordingly, on this record, and under step one of *Alice*, we agree with the Examiner's conclusion the claims are directed to an abstract idea.

Alice Step 2 —Inventive Concept

If the claims are directed to a patent-ineligible concept, as we conclude above, we proceed to the "inventive concept" step. For that step we must "look with more specificity at what the claim elements add, in order to determine 'whether they identify an 'inventive concept' in the application of the ineligible subject matter' to which the claim is directed." *Affinity Labs*, 838 F.3d at 1258 (quoting *Elec. Power Grp.*, 830 F.3d at 1353).

In applying step two of the *Alice* analysis, our reviewing court guides we must "determine whether the claims do significantly more than simply describe [the] abstract method" and thus transform the abstract idea into patentable subject matter. *Ultramercial, Inc. v. Hulu, LLC*, 772 F.3d 709, 715 (Fed. Cir. 2014). We look to see whether there are any "additional features" in the claims that constitute an "inventive concept," thereby rendering the claims eligible for patenting even if they are directed to an abstract idea. *Alice*, 134 S. Ct. at 2357. Those "additional features" must be more than "well-understood, routine, conventional activity." *Mayo*, 566 U.S. at 79.

The Examiner concludes:

> The additional element(s) or combination of elements in the claims other than the abstract idea per se amount(s) to no more than: mere instructions to implement the idea on a computer. Viewed as a whole, these additional claim element(s) do not provide meaningful limitation(s) to transform the abstract idea into a patent eligible application of the abstract idea such that the claim(s) amounts to significantly more than the abstract idea itself.

Ans. 4. Further, under Step 2 of the *Mayo* test, the Examiner concludes the additional limitations, e.g., "encrypting," "sending . . . data," "receiving . . .

ciphertext . . . and decrypting . . . [the ciphertext] to create plaintext . . . [that] is a result of homomorphic operations performed . . . using the encrypted multiple data and the public key," are merely conventional and thus, either alone or in combination, do not amount to significantly more than the judicial exception. Ans. 5.

Appellants point to their Specification as supporting the idea that the claims offer "significantly more" than the abstract idea itself.

> The instant claims are directed to an improvement in computer-related technology. As described in Applicant's specification (see page 6, line 30 to page 7, line 3):
>
> > One of the optimizations is a key-generation method for the underlying somewhat homomorphic encryption, that does not require full polynomial inversion. This reduces the asymptotic complexity from $\tilde{O}(n^{2.5})$ to $\tilde{O}(n^{1.5})$ when working with dimension- n lattices (and practically reducing the time from many hours/days to a few seconds/minutes) . . . .
>
> That is, the key-generation method, which is claimed in part in independent claim 1 and the other independent claims herein, reduces complexity from ***many hours/days* to a few seconds/ minutes**. The subject matter in the instant claims is also an improvement to homomorphic encryption techniques that were available at the time. Consequently, the instant claims are directed to an improvement in computer-related technology.

App. Br. 13.

In the Reply Brief, Appellants continue their argument by contending:

> [Claim 1] is not simply a collection of random components that implement some idea; this is instead a concrete example of encrypted communication . . . . [T]he algorithm allows the encrypted communication to occur . . . [because,] without the algorithm, **there is no encryption and therefore no encrypted**

> **communication**. This is further illustrated by the complete claim 1.

Reply Br. 8. In summary, Appellants argue, "the instant claims . . . recite subject matter that allows encrypted communication to occur and without which there is no encrypted communications. These claims create a physical result—a secure communication." Reply Br. 10.

Evaluating representative claim 1 under step 2 of the *Alice* analysis and for the reasons stated above by Appellants, we are persuaded by Appellants' argument and analysis that the claim is directed to an inventive concept that transforms the abstract idea of "collecting information and using mathematical procedure for converting one form of numerical representation to another" (Final Act. 3) into a patent-eligible application of that abstract idea, i.e., a homomorphic encryption/decryption scheme that improves the underlying encryption and decryption technology.

Accordingly, on this record, we are persuaded of error in the Examiner's conclusion that the appealed claims are directed to patent-ineligible subject matter. Therefore, we do not sustain the Examiner's § 101 rejection of independent claims 1, 8, and 14, and grouped claims 2–7, 9–13, and 15–20, that stand therewith. *See* Claim Grouping, *supra*.

CONCLUSION

The Examiner erred with respect to the patent-eligible subject matter rejection of claims 1–20 under 35 U.S.C. § 101, and we do not sustain the rejection.

DECISION

We reverse the Examiner's decision rejecting claims 1–20.

REVERSED