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.
14/733,795	06/08/2015	Jason Jenks	0097749-445US1	3962

113507 7590 07/01/2020

Davis Wright Tremaine LLP - ATI
IP Docketing Dept.
920 Fifth Ave., Suite 3300
Seattle, WA 98104-1610

EXAMINER	
HUANG, JAY	

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
07/01/2020	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):

amznpatents@dwt.com
patentdocket@dwt.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte JASON JENKS, BRANDON B. LOW, HANSON CHAR, PETER S. VOSSHALL, and WAYLON BRUNETTE

Appeal 2019-004782
Application 14/733,795
Technology Center 3600

Before ST. JOHN COURTENAY III, LARRY J. HUME, and PHILLIP A. BENNETT, *Administrative Patent Judges.*

BENNETT, *Administrative Patent Judge.*

DECISION ON APPEAL

STATEMENT OF THE CASE

Pursuant to 35 U.S.C. § 134(a), Appellant[1] appeals from the Examiner's decision to reject claims 1–5 and 13–22. Claims 6–12 have been withdrawn from consideration. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm in part.

---

[1] We use the word "Appellant" to refer to "applicant" as defined in 37 C.F.R. § 1.42(a). Appellant identifies the real party in interest as Amazon Technologies, Inc. Appeal Br. 3.

CLAIMED SUBJECT MATTER

Appellant describes the invention as relating to "secure decryption and business rule validation of encrypted confidential data within a hardware security module (HSM)." Spec., Abstract. The Specification states "[d]ata validation . . . typically involves testing against a list of valid items or algorithms." Spec. 2.

Claim 1, reproduced below, is illustrative of the claimed subject matter:

> 1. A method comprising:
>
> receiving, at a hardware security module, an application programming interface call to validate data, the application programming interface call made to an application programming interface provided by the hardware security module, the application programming interface call specifying a secret comprising encrypted information from a storage device external to the hardware security module, the hardware security module comprising a
>
> cryptographic processor and memory within a tamper resistant physical package; and
>
> fulfilling the application programming interface call by at least:
>
> decrypting the secret within the hardware security module to obtain cleartext that represents the data;
>
> generating, based at least in part on application of a hashing algorithm to the cleartext within the hardware security module, a validation result that indicates whether the cleartext satisfies a set of rules in the memory corresponding to a type of payment information; and
>
> providing the validation result.

Appeal Br. 25 (Claims Appendix).

REFERENCES

The prior art relied upon by the Examiner as evidence is:

Name	Reference	Date
Ginter et al.	US 2002/0112171 A1	Aug. 15, 2002
Wright et al.	US 2002/0194119 A1	Dec. 19, 2002
Wah et al.	US 2006/0085333 A1	April 20, 2006
Crosson Smith	US 7,236,957 B2	June 26, 2007
Sako et al.	US 2007/0237136 A1	Oct. 11, 2007
Schuba et al.	US 2008/0071903 A1	March 20, 2008

REJECTIONS[2]

Claims 1–3, 13, 15–18, and 20 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Wah, Ginter, and Smith. Final Act. 12.

Claims 4, 5, and 19 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Wah, Ginter, Smith, and Wright. Final Act. 17.

Claim 14 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Wah, Ginter, Smith, and Schuba. Final Act. 19.

Claims 21 and 22 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Wah, Ginter, Smith, and Sako. Final Act. 20.

STANDARD OF REVIEW

The Board conducts a limited *de novo* review of the appealed rejections for error based upon the issues identified by Appellant and in light of the arguments and evidence produced thereon. *Ex parte Frye*, 94 USPQ2d 1072, 1075 (BPAI 2010) (precedential).

[2] The Examiner has withdrawn the rejection of claims 1–5 and 13–22 under 35 U.S.C. § 101. Ans. 3.

ISSUES

We have reviewed Appellant's arguments presented in the Appeal Brief and the Reply Brief. Based on the presented arguments, we identify the following issues for our review:

First Issue: Has the Examiner erred in combining the teachings of Wah with those of Ginter and Smith to teach or suggest the invention recited in claims 1 and 13?

Second Issue: Has the Examiner erred in combining the references in order to teach or suggest "providing the results in a randomized order," as recited in dependent claims 21 and 22?

ANALYSIS

First Issue

In rejecting claim 1, the Examiner relies on the combination of Wah, Ginter, and Smith. Relevant to this issue, the Examiner finds the limitation "generating, based at least in part on application of a hashing algorithm to the cleartext within the hardware security module, a validation result that indicates whether the cleartext satisfies a set of rules in the memory corresponding to a type of payment information" taught or suggested by the combination of Wah, Ginter, and Smith. In particular, the Examiner finds Smith teaches "generating, based at least in part on application of a hashing algorithm to the cleartext, a validation result," while Ginter teaches the recited "within the hardware security module." Final Act. 13–15. The Examiner relies on Wah for teaching "a validation result that indicates whether the cleartext satisfies a set of rules in the memory corresponding to a type of payment information."

In combining Ginter with Wah, the Examiner finds:

> [I]t would have been recognized by those of ordinary skill in the art that modifying the module so it is a hardware security module that receives an API call to decrypt encrypted data, the hardware security module comprising a cryptographic processor and memory within a tamper resistant physical package, results in an improved invention because applying said technique ensures that only authorized entities have access to encrypted data, thus improving the overall security of the invention.

Final Act. 14. In combining Smith with Ginter, the Examiner finds:

> One of ordinary skill in the art would have recognized that applying the known technique of *Smith* to the known invention of *Wah*, *Ginter* would have yielded predictable results and resulted in an improved invention. It would have been recognized that the application of the technique would have yielded predictable results because the level of ordinary skill in the art demonstrated by the references applied shows the ability to incorporate such cryptography features into a similar invention. Further, it would have been recognized by those of ordinary skill in the art that modifying the step of generating a validation result so it uses a hashing algorithm results in an improved invention because applying said technique leverages the SHA-1 hashing algorithm that is known for being secure, thus improving the overall security of the invention.

Final Act. 15.

Appellant argues the Examiner has relied on impermissible hindsight in combining Smith with Ginter and Wah (Appeal Br. 15–22, Reply Br. 3–8) with respect to the "generating" step. Appellant contends the Examiner failed to provide evidence that Smith "contains a known technique that is applicable to a device analogous to a 'hardware security module.'" Appeal Br. 16.

We are not persuaded the Examiner's rationale to combine the cited references is insufficient. With respect to hindsight, Appellant has not

identified knowledge gleaned only from the present application that was not within the level of ordinary skill at the time the claimed invention was made. *See In re McLaughlin*, 443 F.2d 1392 (CCPA 1971). Nor has Appellant provided any objective evidence of secondary considerations (e.g., unexpected results), which our reviewing court guides "operates as a beneficial check on hindsight." *Cheese Sys., Inc. v. Tetra Pak Cheese & Powder Sys., Inc.*, 725 F.3d 1341, 1352 (Fed. Cir. 2013).

Appellant's argument regarding Smith is also unavailing. As noted above, Appellant also contends the Examiner erred in finding that the SHA-1 hashing algorithm described by Smith was "well-known" because it was not officially noticed, nor properly based upon common knowledge. Appeal Br. 17–18. We are not persuaded by Appellant's argument because the Background section of Smith describes the SHA-1 hash as "a well-known secure hash algorithm developed by the National Institute of Standards and Technology which is useful for generating a 160-bit has of any data file. . . ." Smith, col. 2, ll. 12–14. In fact, Appellant's own Specification supports that algorithms were known to be used in data validation, describing: "Data validation . . . typically involves testing against a list of valid items or algorithms." Spec. 2. As such, a preponderance of evidence in the record supports the Examiner's finding.

For the same reasons, we also find unpersuasive Appellant's similar basis for arguing that Smith renders Wah and Ginter unsatisfactory for its intended purpose and changes its principle of operation. Appeal Br. 18–21.

Accordingly, we are not persuaded of Examiner error with respect to the rejection of claims 1 and 13.

Second Issue

Claims 21 and 22, which depend from claims 1 and 13, respectively, recite the limitation that the application programming interface call is fulfilled by "generating a plurality of validation results that corresponds to the plurality of secrets and providing the plurality of validation results in a randomized order." Appeal Br. 28–29 (Claims Appendix). The Examiner relies on Sato for teaching or suggesting the limitation "providing the results in a randomized order." Final Act. 20–21. The Examiner states his motivation to combine the references Wah, Ginter, Smith and Sato was that

> those of ordinary skill in the art that modifying the invention to provide the plurality of results in a randomized order results in an improved invention because applying said technique ensures that nefarious entities will not be able to gain information about the plurality of secrets by intercepting the order of the plurality of results, thus improving the overall security of the invention.

Final Act. 21.

Appellant argues "providing results 'in a randomized order,' by definition means providing results in an 'order' that is unpredictable." Appeal Br. 23. Appellant further argues "The Office cites *Sako* as allegedly teaching this feature, yet fails to explain how *Sako* would be capable of "providing [a plurality of] results in a randomized order" if *Wah* in view of *Ginter*, and further in view of *Crosson Smith* only disclose 'generating a [single] validation result."' Appeal Br. 23.

Appellant argues the Examiner used impermissible hindsight to make the combination of references:

> In fact, despite the Office's declaration that the motivation for combining *Wah, Ginter,* and *Crosson Smith* with *Sako* would be to "ensure[] that nefarious entities will not be able to gain information about the plurality of secrets by intercepting the

> order of the plurality of results, thus improving the overall security of the invention," this motivation appears to have been appropriated from Appellant's specification since the cited portions of the art supply no such motivation. In fact, the reason given by *Sako* for randomizing the order of its "music contents" is so as not to "bore the user" (e.g., by providing music contents to the user in the same order as provided in the past). A person having ordinary skill seeking to foil "nefarious entities" and "improv[e] the overall security of the invention," as proposed by the Office, would not be led to combine the boredom-avoidance technique of *Sako* with the credit card payment system of *Wah* in view of *Ginter,* and further in view of *Crosson Smith.* Therefore, it seems clear that the Office has again resorted to impermissible hindsight to make the combination.

Reply Br. 10–11 (footnotes omitted). We agree with Appellant because, for example, the Sato reference is not in the same field of the invention – it is in the music content field. The section of Sato the Examiner cites teaches transmitting music content in a random order so as not to bore with user with the same, repetitive order of music content. Sako ¶ 135. On this record, we do not find someone of ordinary skill in the art would have considered Sato's transmission of randomized music content as a teaching or suggestion to provide the validation results in a randomized order to thwart a security risk.

As such, we are persuaded the Examiner has erred in rejecting claims 21 and 22.

Remaining Claims

Appellant does not present separate arguments for the remaining rejected claims. Appeal Br. 23–24. Therefore, we sustain the rejections of claims 2–5 and 14–20 under 35 U.S.C. § 103(a).

CONCLUSION

The Examiner's rejection is affirmed in part.

More specifically:

We reverse the Examiner's rejection of claims 21 and 22 under 35 U.S.C. § 103(a).

We affirm the Examiner's rejections of claims 1–5 and 13–20 under 35 U.S.C. § 103(a).

DECISION SUMMARY

Claims Rejected	**35 U.S.C. §**	**Reference(s)/Basis**	**Affirmed**	**Reversed**
1–3, 13, 15–18, and 20	103(a)	Wah, Ginter, and Smith	1–3, 13, 15–18, and 20	
4, 5, and 19	103(a)	Wah, Ginter, Smith, and Wright	4, 5, and 19	
14	103(a)	Wah, Ginter, Smith, and Schuba	14	
21 and 22	103(a)	Wah, Ginter, Smith, and Sako		21 and 22
Overall Outcome			1–5 and 13–20	21 and 22

TIME PERIOD FOR RESPONSE

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

AFFIRMED IN PART