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.
15/436,489	02/17/2017	Donald STARK	2332100US	8114

149118 7590 09/15/2020

Colby Nipper / Google
291 East Shore Drive
Suite 200
Eagle, ID 83616

EXAMINER	
KORSAK, OLEG	

ART UNIT	PAPER NUMBER
2492	

NOTIFICATION DATE	DELIVERY MODE
09/15/2020	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):

docket@colbynipper.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte DONALD STARK

Appeal 2020-004523
Application 15/436,489
Technology Center 2400

Before JOSEPH L. DIXON, JAMES R. HUGHES, and JOHN A. EVANS, *Administrative Patent Judges*.

HUGHES, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

Claims 29–57 are pending, stand rejected, are appealed by Appellant,[1] and are the subject of our decision under 35 U.S.C. § 134(a). *See* Final Act. 1–2; Appeal Br. 5.[2] We have jurisdiction under 35 U.S.C. § 6(b).

We REVERSE.

---

[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 Google, Inc. *See* Appeal Br. 3.

[2] We refer to Appellant's Specification ("Spec."), filed Feb. 17, 2017 (claiming benefit of US 62/298,842 (filed Feb. 23, 2016)); and Appeal Brief ("Appeal Br."), filed Sept. 12, 2019. We also refer to the Examiner's Final Office Action ("Final Act."), mailed Apr. 15, 2019; and Answer ("Ans.") mailed Nov. 22, 2019.

CLAIMED SUBJECT MATTER

The invention "generally relates to methods and [apparatuses] for protecting the security of data" and more "specifically, . . . to protecting against cryptographic attacks using clock period randomization." Spec. ¶ 7. The method recites a process of generating a variable clock signal with a variable clock period for use during a cryptographic operation that includes receiving an input clock signal, generating a fixed delay, generating a variable delay, combining the fixed and variable delays to create a combined delay, applying the combined delay to the input clock signal to create the variable clock period, and generating the variable clock signal from the variable clock period. *See* Spec. ¶ 8; Abstract. Claims 29 (directed to a method) and 44 (directed to an apparatus) are independent. Claim 29, reproduced below, is illustrative of the claimed subject matter:

> 29. A method of generating a variable clock signal with a variable clock period for use during a cryptographic operation, the method comprising:
>
> receiving an input clock signal;
>
> generating a fixed delay amount;
>
> *generating a variable delay amount*;
>
> *combining the fixed delay amount and the variable delay amount to create a combined delay amount*;
>
> *applying the combined delay amount to the input clock signal to create the variable clock period*; and
>
> generating the variable clock signal based on the variable clock period to control a device during the cryptographic operation.

Appeal Br. 40 (Claims App.) (emphasis added).

REFERENCES

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

Name	Reference	Date
Lin	US 2009/0163166 A1	June 25, 2009
Samavedam et al. ("Samavedam")	US 2011/0074509 A1	Mar. 31, 2011
Henry et al. ("Henry")	US 2011/0296202 A1	Dec. 1, 2011
Xu et al. ("Xu")	US 2013/0285729 A1	Oct. 31, 2013

Bayrak et al., *An EDA-Friendly Protection Scheme against Side-Channel Attacks*, EDAA (2013) ("Bayrak").

Bialek et al., *Implementation of a Digital Trim Scheme for SAR ADCs*, 11 Adv. Radio Sci., 227–230 (2013) ("Bialek").

REJECTIONS[3]

1. The Examiner rejects claims 30, 34, 41, 45, 50, and 55 under 35 U.S.C. § 112(a) as failing to comply with the written description requirement.[4] *See* Final Act. 2–4; Ans. 4–8.

2. The Examiner rejects claims 29–32, 34–36, 38, 44–48, 50, and 51 under 35 U.S.C. § 102(a)(1) as being anticipated by Bayrak. *See* Final Act. 4–7.

[3] The Leahy-Smith America Invents Act ("AIA"), Pub. L. No. 112–29, 125 Stat. 284 (2011), amended 35 U.S.C. §§ 102, 112, and 103. Because the present application has an effective filing date (Feb. 23, 2016) after the AIA's effective date, this decision refers 35 U.S.C. §§ 102(a)(1), 112(a), and 103.

[4] The Examiner also rejected claims 33, 35, 48, and 49 under 35 U.S.C. § 112(a) (*see* Final Act. 3–4), but withdrew the rejection of these claims (*see* Ans. 4). We do not address Appellant's arguments with respect to the withdrawn rejection.

3. The Examiner rejects claims 33 and 49 under 35 U.S.C. § 103 as being unpatentable over Bayrak and Henry. *See* Final Act. 7–8.

4. The Examiner rejects claims 37, 39, 52, and 53 under 35 U.S.C. § 103 as being unpatentable over Bayrak and Lin. *See* Final Act. 8–9.

5. The Examiner rejects claims 40, 41, 54, and 55 under 35 U.S.C. § 103 as being unpatentable over Bayrak and Samavedam. *See* Final Act. 10.

6. The Examiner rejects claims 42 and 56 under 35 U.S.C. § 103 as being unpatentable over Bayrak, Samavedam, and Xu. *See* Final Act. 11.

7. The Examiner rejects claims 43 and 57 under 35 U.S.C. § 103 as being unpatentable over Bayrak, Samavedam, Xu, and Bialek. *See* Final Act. 11.

ANALYSIS

Written description Rejection of Claims 30, 34, 41, 45, 50, and 55

The Examiner rejects dependent claims 30, 34, 41, 45, 50, and 55 as failing to comply with the written description requirement. *See* Final Act. 2–4; Ans. 4–8. Specifically, the Examiner rejects claims 30 and 45 because the claims recite "another variable clock period" (Final Act. 3 (emphasis omitted)), for which the Examiner finds no written description support in Specification. *See* Final Act. 3; Ans. 5–6. The Examiner also rejects claims 34 and 50 because the claims recite "prevents a fault injection attack" (Final Act. 3 (emphasis omitted)), for which the Examiner finds no written description support in Specification. *See* Final Act. 3; Ans. 7. The Examiner further rejects claims 41 and 55 because the claims recite "linear capacitors are activated or deactivated prior to generating the variable delay

amount" (Final Act. 4 (emphasis omitted)), for which the Examiner, again, finds no written description support in Specification. *See* Final Act. 4; Ans. 8.

Appellant contends that support for the disputed features of claims 30 and 45—"another variable clock period" (quoting claim 30 (Appeal Br. 41 (Claims App.))—"can be found in at least FIG. 2 and [0008] of the . . . specification." Appeal Br. 14; *see* Appeal Br. 14–15 (citing Spec. ¶ 8; Fig. 2). Appellant also contends that the disputed features of claims 34 and 50—"prevents a fault injection attack" (quoting claim 34 (Appeal Br. 41 (Claims App.)))—are supported by the Specification. *See* Appeal Br. 16 (citing Abstract). Appellant further contends that support for the disputed features of claims 41 and 55—"linear capacitors are activated or deactivated prior to generating the variable delay amount" (quoting claim 41 (Appeal Br. 43 (Claims App.))—"can be found in at least [0083] of the . . . specification. Appeal Br. 17 (citing Spec. ¶ 83).

The test for sufficiency under the written description requirement "is whether the disclosure of the application relied upon reasonably conveys to those skilled in the art that the inventor had possession of the claimed subject matter as of the filing date." *Ariad Pharms, Inc. v. Eli Lilly and Co.*, 598 F.3d 1336, 1351 (Fed. Cir. 2010).

With respect to claims 30 and 45, Appellant's cited support (Spec. ¶ 8; Fig. 2) describes a process for generating a variable clock period and multiple variable clock periods. Further, Figure 2 and the Specification provide a detailed explanation of generating multiple variable clock periods. *See* Spec. ¶¶ 40, 60–61; Fig. 2. We find the above-described subject matter from Appellant's Specification provides sufficient written description

support for the claimed features the Examiner found lacking in such support. We, therefore, find the Examiner erred in rejecting claims 30 and 45 as lacking sufficient written description support.

With respect to claims 34 and 50, Appellant's cited support (Abstract) does not explicitly describe preventing a fault injection attack (the prevention of all possible fault injection attacks), but does describe a process that makes "fault injection attacks more difficult by using a clock with a variable period during a cryptographic operation" (Abstract). As discussed *supra*, Appellant's Specification provides a detailed explanation of generating variable clock periods (*see* Spec. ¶¶ 40, 60–61; Fig. 2) which makes such attacks more difficult (i.e., less likely to succeed—that is, the process lessens the probability of an attack succeeding). *See* Spec. ¶¶ 54, 56. 58, 60, 62, 71. We agree with Appellant that making an attack more difficult or less likely to succeed at least suggests (to one of ordinary skill in the art) preventing an attack, and, therefore, would have reasonably conveyed that Appellant had possession of the claimed subject matter to one of ordinary skill in the art. We find the above-described subject matter from Appellant's Specification provides sufficient written description support for the claimed features the Examiner found lacking in such support. Thus, we find the Examiner erred in rejecting claims 34 and 50 as lacking sufficient written description support.

With respect to claims 41 and 55, Appellant's cited support (Spec. ¶ 83) does not explicitly describe that the linear capacitors are activated (or deactivated) prior to generating the variable delay, but does describe a process for activating (deactivating) the capacitors—"the control signals to capacitors 440a-440d may operate one or more switches that switch

capacitors 440a-440d into/out of the circuit" (Spec. ¶ 83). In particular, the above description shows Appellant had possession of activating or deactivating the capacitors. *See* Spec. ¶ 83; Fig. 10. It follows from claims 29, 32, 36, 38, and 40, on which claim 41 depends, and Appellant's Specification that activating the capacitors must precede generating the variable delay that requires the use of delay generators that comprise banks of the linear capacitors. *See* claims 29, 32, 36, 38, 40, and 41 (Appeal Br. 40–43 (Claims App.)); *see also* Spec. ¶¶ 9, 13, 24, 67, 75, 76, 83, 87, 88. We, therefore, conclude the Examiner erred in rejecting independent claims 41 and 55 as lacking sufficient written description support.

Anticipation Rejection of Claims 29–32, 34–36, 38, 44–48, 50, and 51

The Examiner rejects independent claim 29 (as well as independent claim 44, and dependent claims 30–32, 34–36, 38, 45–48, 50, and 51) as being anticipated by Bayrak. *See* Final Act. 4–7; Ans. 9–14. Appellant contends that Bayrak does not disclose the disputed limitations of claim 29. *See* Appeal Br. 18–21. Specifically, Appellant contends, *inter alia*, that the cited portions of Bayak (disclosing "τ_{prot}" and "M random clocks") "cannot both be analogous to the 'combined delay amount' of claim 29" and that "one of the 'M random clocks' of Bayrak cannot be analogous to both the 'variable delay amount' and the 'combined delay amount' of claim 29." Appeal Br. 19; *see* Appeal Br. 17–21.

We agree with Appellant that the Examiner-cited portions of Bayrak (*see* Bayrak 2 and Fig. 2) do not explicitly or inherently describe the generating a fixed delay and a variable delay and combining the fixed and variable delay to create a combined delay that is then applied to the input

clock signal to create a variable clock period, as required by Appellant's claim 29. *See* Appeal Br. 17–21. Specifically, Bayrak describes "τ_{prot}" that is a clock period (*see* description of Fig. 2 on page 2) and "M random clocks" that are generated random clocks (*see* Bayak Section II and description of Fig. 2 on page 2), and that the phase-shifted clock signals (having the increased clock period (τ_{prot}) are multiplexed to generate the randomized clocks (M random clocks). Although Bayrak describes randomized variable clock generation (Bayrak 2), it is unclear from the Examiner's rejection how Bayrak's generated randomized clocks (M random clocks) can be combined with a variable delay to create a combined delay when Bayrak's "M random clocks" are the resulting variable clock signal (the "variable clock signal based on the variable clock period" recited in claim 29). The Examiner appears to misconstrue the disclosure of the Bayrak reference and when properly interpreted the Examiner-cited portions of Bayrak cannot logically disclose the process of generating the variable clock signal recited in claim 29.

Consequently, we are constrained by the record before us to find that the Examiner erred in finding Bayrak anticipates Appellant's claim 29. Independent claim 44 includes limitations of commensurate scope. Claims 30–32, 34–36, 38, 45–48, 50, and 51 depend from and stand with their respective base claims. Accordingly, Appellant's contentions persuade us of error in the Examiner's anticipation rejection of claims 29–32, 34–36, 38, 44–48, 50, and 51, and we reverse the Examiner's rejection of these claims.

Obviousness Rejections of Claims 33, 37, 39–43, 49, and 52–57

The Examiner rejects claims 33, 37, 39–43, 49, and 52–57 under 35 U.S.C. § 103 as being unpatentable over the cited prior art. Specifically, the Examiner rejects claims 33 and 49 over Bayrak and Henry (*see* Final Act. 7–8); the Examiner rejects claims 37, 39, 52, and 53 over Bayrak and Lin (*see* Final Act. 8–9); the Examiner rejects claims 40, 41, 54, and 55 over Bayrak and Samavedam (*see* Final Act. 10); the Examiner rejects claims 42 and 56 over Bayrak, Samavedam, and Xu (*see* Final Act. 11); and the Examiner rejects claims 43 and 57 over Bayrak, Samavedam, Xu, and Bialek (*see* Final Act. 11). The Examiner does not suggest the additional cited references (Henry, Lin, Samavedam, Xu, and Bialek), alone or in combination, cure the above noted deficiencies of Bayrak (*supra*). Therefore, we reverse the Examiner's obviousness rejections of dependent claims 33, 37, 39–43, 49, and 52–57 for the same reasons set forth for claim 29 (*supra*).

CONCLUSION

Appellant has shown that the Examiner erred in rejecting claims 30, 34, 41, 45, 50, and 55 under 35 U.S.C. § 112(a). Appellant has also shown that the Examiner erred in rejecting claims 29–32, 34–36, 38, 44–48, 50, and 51 under 35 U.S.C. § 102(a)(1). Appellant has further shown that the Examiner erred in rejecting claims 33, 37, 39–43, 49, and 52–57 under 35 U.S.C. § 103. We, therefore, do not sustain the Examiner's rejections of claims 29–57.

DECISION SUMMARY

In summary:

Claims Rejected	35 U.S.C. §	Reference(s)/ Basis	Affirmed	Reversed
30, 34, 41, 45, 50, 55	112(a)	Written Description		30, 34, 41, 45, 50, 55
29–32, 34–36, 38, 44–48, 50, 51	102(a)(1)	Bayrak		29–32, 34–36, 38, 44–48, 50, 51
33, 49	103	Bayrak, Henry		33, 49
37, 39, 52, 53	103	Bayrak, Lin		37, 39, 52, 53
40, 41, 54, 55	103	Bayrak, Samavedam		40, 41, 54, 55
42, 56	103	Bayrak, Samavedam, Xu		42, 56
43, 57	103	Bayrak, Samavedam, Xu, Bialek		43, 57
Overall Outcome				**29–57**

REVERSED