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.
14/804,286	07/20/2015	Hugues de Perthuis	81639023US02	1059

65913 7590 09/01/2020

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

EXAMINER	
LEMMA, SAMSON B	

ART UNIT	PAPER NUMBER
2498	

NOTIFICATION DATE	DELIVERY MODE
09/01/2020	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):

ip.department.us@nxp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte HUGUES DE PERTHUIS

Appeal 2019-002290
Application 14/804,286
Technology Center 2400

Before JEFFREY S. SMITH, ADAM J. PYONIN, and AMBER L. HAGY, *Administrative Patent Judges.*

HAGY, *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 1–13, 15, and 16, which are all of the

---

[1] We use the word Appellant to refer to "applicant" as defined in 37 C.F.R. § 1.42. Appellant's Appeal Brief does not expressly identify the real party-in-interest, but NXP B.V. is identified as the Applicant in the record before us. *See* Bib Data Sheet; MPEP 1205 (The Appeal Brief shall contain "[a] statement identifying by name the real party in interest at the time the appeal brief is filed, except that such statement is not required if the named inventor or inventors are themselves the real party in interest.").

pending claims.[2] *See* Final Act. 1. We have jurisdiction under 35 U.S.C. § 6(b).

We REVERSE.

CLAIMED SUBJECT MATTER

According to Appellant, the present Application describes and claims "methods of encrypting and decrypting blocks of data stored in computer readable memory for a microprocessor using a block cipher with a nonce," wherein "the value of the nonce is based on previous execution instructions of a program executed by the microprocessor for a previously encrypted block." *Id.* at 1:5–10.

Claims 1, 9, 15, and 16 are independent. Claim 1, reproduced below with the disputed limitation italicized, represents the claimed subject matter:

> 1. A method of encrypting blocks of data bits stored in a computer readable memory for a device using a block cipher with a nonce and a key, the method comprising for each block of data:
>
> generating a value of the nonce based on previous execution instructions of a program executed by the device for a previously executed block of data, wherein integrity of execution flow is tied to the generated value of the nonce such that a decryption error will occur and stop processing after an execution flow disruption attack *and the generated value of the nonce depends upon an address of a previous instruction executed by the device*;
>
> and encrypting the block of data with the nonce and the key using the block cipher.

Appeal Br. 11 (Claims App'x).

---

[2] Claim 14 has been canceled. *See* Appeal Br. 14 (Claims App'x); Final Act. 1.

REJECTION

The Examiner rejects all pending claims (claims 1–13, 15, and 16) under 35 U.S.C. § 102(a) as anticipated by Matthews, U.S. Application No. 2011/0085657 A1, published April 14, 2011 ("Matthews"). Final Act. 5–14.

OPINION

For essentially the reasons argued by Appellant (Appeal Br. 5–6; Reply Br. 1–2), we are persuaded of Examiner error in the finding that Matthews' generated seed value, which the Examiner finds discloses the claimed "nonce," "depends upon an address of a previous instruction executed by the device," as recited in claim 1 and commensurately recited in independent claims 9, 15, and 16. *See* Final Act. 6–8.

As support for finding that Matthews discloses the disputed limitation, the Examiner cites to Matthews' disclosure of an encoded block of data serving as a seed for encoding a subsequent block of data, and so on until all blocks of input data are encoded. *Id.* at 7 (citing Matthews ¶¶ 49–51). However, as Appellant points out, and we agree, the cited disclosure of Matthews does not describe the seed value as depending on an address of a *previously executed instruction*. Appeal Br. 5. Rather, as Appellant notes, "the seed value of Matthews is 'derived from a count value indicative of the number of times a write access has occurred.'" *Id.* (citing Matthews ¶ 68 and Fig. 9).

In the Answer, the Examiner finds Matthews discloses that, in addition to count value, "[t]he seed value can incorporate other variables as well, such as the associated LBA/logical block address (or LBAs) of the input data, a PBA [physical block or sector address] associated with the target page, etc." Ans. 6 (citing Matthews ¶ 45) (emphasis omitted). The

Examiner then states that "the generated value of the nonce/seed is derived from the metadata that contains the count value which depends upon a memory address, logical block address (LBA) or cell or page of the previously carried out write and/or erase operators/instructions executed by the device." *Id.* at 7.

Appellant points out in the Reply that the Examiner has still failed to find that Matthews discloses the seed value / nonce depends upon an *address of a previous instruction executed by the device*. Reply Br. 2. We agree. The only "address" underlying the Examiner's findings regarding Matthews is the *address of input data*. *See* Final Act. 6 (citing Matthews ¶ 45). In that regard, we note that Matthews consistently uses the term "input data" to refer to data "provided for writing to a target page of memory in a storage array." *E.g.*, Matthews, Abstract, Fig. 9, ¶ 2. In other words, the "input data" in Matthews is *data that is to be stored*. In contrast, Appellant's Specification describes generation of a "nonce" in terms of an address of *an instruction being fetched*:

> [A] nonce (an arbitrary number used once) is generated and concatenated to the address of the instruction being fetched, creating a counter value. The same nonce is then concatenated to every address fetched to provide a series of counter values. This provides a series of counter values that are each unique for each address of the instruction and tied to the value of each address.

Spec. 2:1–6. The Examiner does not explain, and we do not discern from the available record, how deriving a seed value from the *address of input data*, as described in Matthews, discloses the "generated value of the nonce depends upon an *address of a previous instruction executed by the device*,"

as claimed here, such that Matthews' disclosure anticipates the claimed invention.

Thus, for the foregoing reasons, we are persuaded of Examiner error in the 35 U.S.C. § 102(a) rejection of independent claims 1, 9, 15, and 16, and we, therefore, do not sustain that rejection. The dependent claims stand with their respective independent claims.[3]

CONCLUSION

The Examiner's 35 U.S.C. § 102(a) rejection of claims 1–13, 15, and 16 is reversed.

DECISION SUMMARY

Claims Rejected	**35 U.S.C. §**	**Reference(s)/Basis**	**Affirmed**	**Reversed**
1–13, 15, 16	102(a)	Matthews		1–13, 15, 16

REVERSED

[3] Appellant's contentions present additional issues. Because the identified issue is dispositive of Appellant's arguments on appeal, we do not reach the additional issues.